2. GENERAL CYBER SECURITY REQUIREMENTS

a. Basic Safeguarding of TSP Information Systems.

(1) In order to protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) created by or used in the TOS, the Government is implementing a phased approach to increasing cybersecurity controls including reporting of cybersecurity breaches.

(2) The phased approach models itself on the Cyber Maturity Model Certification. In order to be awarded any shipments after 15 May 2026, the TSP and any subcontractors possessing FCI or CUI must complete by 15 March 2026 and maintain as current, an affirmation, by the TSP's CEO of continuous compliance with the requirements associated with the CMMC Level 1 self-assessment in the Supplier Performance Risk System (SPRS) (https://piee.eb.mil) for each CMMC unique identifier (UID) applicable to each of the TSP information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract.

(3) In order to be awarded any shipments after 15 May 2027, the TSP and any subcontractors possessing FCI or CUI must complete by 15 March 2027 and then annually thereafter and maintain as current, an affirmation, by the TSP's CEO of continuous compliance with the requirements associated with the CMMC Level 2 self-assessment in the SPRS for each CMMC unique identifier (UID) applicable to each of the TSP information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract.

(4) TSPs shall ensure all subcontractors and suppliers complete prior to subcontract award, and maintain on an annual basis, an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance with the requirements associated with the CMMC level required for the subcontract or other contractual instrument for each of the subcontractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the subcontract.

b. Handling and Protection of Non-Public Information.

(1) CUI means information the Government creates or possesses, or information an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls (32 CFR 2002.4(h)).

(2) Federal contract information (FCI) means information, not intended for public release, that is provided by or generated for the Government under the TOS to develop or deliver a service to the Government. It does not include information provided by the Government to the public, such as on public websites, or simple transactional information, such as information necessary to process payments.

(3) TSPs operating in the TOS have access to CUI, category, GENERAL PRIVACY (PRVCY) information, which refers to personal information, or, in some cases, "personally identifiable information (PII)," as defined in OMB M-17-12, or "means of

identification" as defined in 18 U.S.C. § 1028(d)(7). Examples of PII to which the TSP has access are names of Servicemembers, DoW, USCG employees and their family members, origin and destination addresses, work and personal telephone/mobile phone numbers, social security numbers, DoW Identification Numbers, work and personal email addresses, and electronic household goods inventories including remote surveys and video, and claims related information including banking information provided to pay inconvenience claims or loss/damage claims.

(4) The Contractor agrees to use FCI information developed or received, including CUI while performing under the TOS only for the purposes of fulfilling the contracted requirements and to protect such information from unauthorized release or disclosure. Information may be provided to subcontractors only as needed to perform their subcontracted duties. Such information may not be sold or provided to third-parties or others such as advertisers or data-brokers.

c. The following basic safeguarding requirements and procedures are required to protect TSP information technology systems, including mobile applications, that process information received under the ToS program. IAW 48 CFR 52.204-1 and 32 CFR Part 170, these requirements and procedures for basic safeguarding of TSP systems shall include, at a minimum, the following security controls:[1]

(1) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(2) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(3) Verify and control/limit connections to and use of external information systems.

(4) Control information posted or processed on publicly accessible information systems.

(5) Identify information system users, processes acting on behalf of users, or devices.

(6) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(7) Sanitize or destroy information system media containing HHG ToS information before disposal or release for reuse.

(8) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(9) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(10) Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

[1] These basic requirements are equivalent to CMMC Level 1 (self).

(11) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(12) Identify, report, and correct information and information system flaws in a timely manner.

(13) Provide protection from malicious code at appropriate locations within organizational information systems.

(14) Update malicious code protection mechanisms when new releases are available.

(15) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

d. Cybersecurity Incident Reporting.

(1) "Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. Reportable cyber-incidents (regardless of whether the information system contains CUI or there is an impact to performance such as delivery schedule delay), include, but are not limited to, the following:

(a) Cyber-incidents as defined in Table 2.

(b) Notifications by a federal, state, or local law enforcement agency or cyber-center (i.e., National Cyber Investigative Joint Task Force (NCIJTF), National Cybersecurity & Communications Integration Center (NCCIC)) of being a victim of a successful or unsuccessful cyber-event, anomaly, incident, insider threat, breach, intrusion, or exfiltration.

Table 2.

Incident Category	Description
Root Level Intrusion	Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
User Level Intrusion	Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
Denial of Service	Denial of Service (Incident)—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.
Malicious Logic	Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Root or User Level Intrusion incidents. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.
Ransomware	Malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. Ransomware is a reportable incident that may be associated with multiple incident categories depending on the attack vector and execution.

(2) When a cyber-incident occurs, the contractor is required to notify USTRANSCOM as soon as practical, but no later than 72 hours after discovering a reportable cyber-incident. The reporting timeline begins when the incident is discovered or reported to the company, its employees, contractors, or cybersecurity firm responsible for providing cybersecurity and response for the company. The TSP shall contact the USTRANSCOM Cyber Operations Center (CyOC) via phone at 618-817-4222. If the TSP does not immediately reach the CyOC via phone, the contractor shall send an email notification to transcom.scott.tcj6.mbx.cyoc-dodin-operations@mail.mil.

e. Mandatory Reporting Data.

(1) The TSP shall work with the USTRANSCOM CyOC through resolution of the incident. Within 72 hours of becoming aware of a reportable cyber-incident, the TSP shall provide an initial notification of the incident, even if some details are not yet available, which includes, but is not limited to, the following information:

(a) Company Name

(b) Who will be the POC with contact information

(c) DPMO/JPPSO POCs (names, telephones, email addresses)

(d) Overall Assessment –Description of incident, data at risk, mitigations applied

(e) Indicators of compromise

(f) Vector of attack (if known)

(g) Estimated time of attack (if known)

(2) The TSP shall provide a follow-on cyber-incident report to the USTRANSCOM CyOC within 5 calendar days of becoming aware of a reportable cyber-incident, which includes, but is not limited to, the following information:

(a) TSP unique Commercial and Government Entity (CAGE) code

(b) TSP SCAC

(c) Bill of Lading numbers implicated

(d) Facility CAGE code where the incident occurred if different than the prime TSP location

(e) POC if different than the POC recorded in the System for Award Management (name, address, position, telephone, email)

(f) DPMO/JPPSO POC (name, telephone, email)

(g) Contract clearance level (should be unclassified)

(h) DoD programs, platforms, systems, or information involved

(i) Location(s) of compromise

(j) Date incident discovered

(k) Type of compromise (e.g., unauthorized access, inadvertent release, other)

(l) Description of technical information compromised

(m) Any additional information relevant to the information compromise

f. In addition to the reporting required by paragraph d. and e., when the TSP discovers a cyber incident that affects a TSP IT system containing TOS FCI or CUI, or that affects the contractor's ability to perform the requirements of the contract, the Contractor shall:

(1) Conduct a review for evidence of compromise of FCI/CUI, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered TSP information system(s) that were part of the cyber incident, as well as other information systems on the TSP's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the TSP's ability to provide TOS services; and

(2) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(3) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(4) Medium assurance certificate requirement. In order to report cyber incidents in to DC3, the TSP or its subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

g. Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3.

h. Media preservation and protection. When a TSP discovers a cyber incident has occurred, the TSP shall preserve and protect images of all known affected information systems identified in paragraph 2.f.(1) and all relevant monitoring/packet capture data (information, data, logs, electronic files and similar information (See NIST Special Publication 800-61: Computer Security Incident Handling Guide, (current version)) (for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest. This will permit a subsequent forensic analysis so that an accurate and complete damage assessment can be accomplished by the Government.

i. Incident Reporting Coordination.

(1) In the event of a cyber-incident, the DoD may conduct an on-site review of network or information systems where FCI/CUI information is resident on or transiting to assist the TSP in evaluating the extent of the incident and to share information in an effort to minimize the impact to both parties. Date and time of on-site visits will be mutually agreed upon by USTRANSCOM and the TSP in advance.

(2) The TSP agrees to allow follow-on actions by the Government (e.g., USTRANSCOM, Federal Bureau of Investigation, Department of Homeland Security, DC3) to further characterize and evaluate the suspect activity. The TSP acknowledges that damage assessments might be necessary to ascertain an incident methodology and identify systems compromised because of the incident.

(3) The TSP is not required to maintain an organic forensic capability, but must ensure data is preserved (e.g., remove an affected system, while still powered on, from the network) and all actions documented until forensic analysis can be performed by the Government or, if the Government is unable to conduct the forensic analysis, a mutually agreed upon third party (e.g., Federally Funded Research and Development Center (FFRDC), commercial security TSP). Any follow-on actions shall be coordinated with the TSP via the DPMO.

(4) The TSP agrees to indemnify and hold the government harmless for following any recommendations to remedy or mitigate the cyber-incident following the actions under 2.i.(1) and 2.i.(2).

j. Confidentiality and Non-Attribution Statement**.** The Government may use and disclose reported information as authorized by law and will only provide attribution information on a need-to-know basis to authorized persons for cybersecurity and related purposes (e.g., in support of forensic analysis, incident response, compromise or damage assessments, law enforcement, counterintelligence, threat reporting, and trend analysis). The Government may share threat information with other USTRANSCOM industry partners without attributing or identifying the affected TSP.