INFORMATION TECHNOLOGY SPECIAL PROVISION (March 30, 2022)

(a) The Company has determined that this Agreement requires Seller to use, access, manage, or exchange information that the Company has determined to require protection from unauthorized disclosure. Seller will manage this information on an information system external to the Company. An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components include, but are not limited to, such devices as firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances. Servers include, but are not limited to, database servers, authentication servers, electronic mail and web servers, proxy servers, domain name servers, and network time servers. Media includes, but is not limited to, disks, flash drives, tapes, thumb drives, mobile devices, paper and CD-ROMS. Access to information must be based on need-to-know and all users must be trained to include appropriate protection measures for the type of information processed.

(b) Seller is required to have security controls on its information system and media necessary to adequately protect the information that will be processed by Seller to perform this Agreement, or information that is created by Seller for Company using the guidelines set forth in the current National Institute of Standards and Technology (NIST) Special Publication SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" or equivalent security and privacy controls, for the security category of information that will be processed by Seller to perform this Agreement, or information that is created by Seller for Company. Prior to commencement of this Agreement, Seller is required to certify and submit to Company's Procurement Officer that Seller's information system and media contain adequate security controls for the security category of information that is processed in the performance of this Agreement. If Seller modifies the security configuration of its information system after its certification to Company, Seller must notify the Company of the changes and complete and submit a new certification to Company that the system controls are adequate for the security category of information processed in the performance of this subcontract. If the security category of the information increases from the level that has been approved by Company, Seller must complete and submit to the Company's Procurement Officer a new certification that its information system and media meets the appropriate security controls for the new information security category.

(c) Foreign nationals may be prohibited from having access to certain categories of information provided by the Company.

(d) Upon termination of this Agreement, Seller must remove all information provided by Company from any workstations and servers by method approved by Company. Media containing Company information must be destroyed by method approved by Company. Seller must provide a certification to Company that Company information has been removed from workstations, servers and media. Alternately, media created under this Agreement may be returned to the Company's Procurement Officer.

(e) Unless prior approval is obtained from Company, Seller is prohibited from using a lower-tier subcontractor's information system or information systems that are not under its control. Seller shall include this clause in all of its subcontracts, at any tier, involving performance of this Agreement. However, such provision in the subcontracts shall not relieve Seller of its obligation to assure compliance with the provisions of this clause for all aspects of the work.

(f) Computer passwords must be issued to individuals accessing the Company information and must not be shared. Computer passwords must be protected by Seller personnel or agents to prevent disclosure or potential disclosure of Company information. If password is compromised, Seller personnel or agents must notify Company immediately.

(g) Any events or unusual situations involving Company's information must be reported to the ORNL Laboratory Shift Superintendant at (865) 574-6606 immediately.

(h) Access to Company's information by Seller may be permitted as required to perform this Agreement. Company's information may be accessed only to perform work authorized in this Agreement.

(i) Information or data furnished by Company must be protected by the Seller to prevent disclosure to any person other than Seller's personnel or agents having a need to know unless such disclosure is authorized in writing by Company.

(j) Classified material and information shall be protected in accordance with the security provisions of this Agreement, if applicable. All classified processing under this Agreement must be on certified and accredited systems. If this Agreement does not include security provisions and the Seller is furnished or comes into contact with classified material or information, it shall be reported immediately to ORNL Laboratory Shift Superintendent at (865) 574-6606.

(k) Seller mobile computing resources used to support this Agreement must contain appropriate security controls. Seller should refer to the NIST 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise

(l) Seller computing resources used to perform this Agreement are subject to audit of the pertinent items by Company Cyber Security.

(m) The Seller agrees to protect all PII in accordance with applicable Federal, State, and other regulatory requirements for the collection, use, and protection of personally identifiable information.