

## INFORMATION TECHNOLOGY SPECIAL PROVISION (June 2008)

(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, 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 that meet the appropriate National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 1, 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 Cyber Security Point of Contact that Seller's information system and media meet the baseline security controls of NIST 800-53 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, complete and submit a new NIST 800-53 certification to Company. 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 Cyber Security Point of Contact a new NIST 800-53 certification that its information system and media meet the baseline security controls of NIST 800-53 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.

(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 their 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.