1. DEFINITIONS

Cyber Asset (CA) — consists of or contains an electronic device that:

a) has communication ports;
b) has programming ports;
c) has wireless capability;
d) accepts removable media;
e) has a human machine interface that can be used to affect availability, integrity, or confidentiality; or
f) has a microprocessor or programmable logic item that can be feasibly reprogrammed after manufacturing.

Cyber Essential Asset (CEA) — a cyber asset that performs or affects:

a) functions important to nuclear safety;
b) nuclear security functions;
c) emergency preparedness functions;
d) safeguard functions; or
e) auxiliary systems which could adversely affect Items a) to d).

Cyber Equipment — any computing hardware, software, firmware or other computing technology (other than a Cyber Essential Asset) that is connected to any NB Power network or is used to access, create, modify, store, process or transmit NB Power Data in the course of performing Contractor's obligations under this Agreement.

Cyber Services — any application, infrastructure or related service provided by any Contractor in relation to any asset designated by NB Power as a Cyber Essential Asset.

2. CYBER SECURITY REQUIREMENTS

Contractor:

2.1 represents and warrants to NB Power that: (i) Contractor has a written and enforceable cyber security policy, and has established and maintains a cyber security program that is designed and implemented to prevent, detect and respond to cyber incidents that may adversely affect NB Power CEAs; and (ii) Contractor's personnel (which, for the purposes of these requirements, includes any Contractor personnel having access to NB Power CEAs) have completed position-appropriate cyber security training;

2.2 shall immediately revoke all access to NB Power CEAs for any Contractor's personnel who is terminated or no longer needs access to NB Power CEAs;

2.3 shall notify NB Power after discovering any security breach, incident or vulnerability affecting or otherwise involving NB Power CEAs. Contractor shall also provide to NB Power, a description of the breach, incident or vulnerability, its potential security impact, its cause, a remediation plan, and recommended mitigating or corrective actions;

2.4 shall: (i) ensure that any CEAs supplied do not contain malware, adware, spyware; and (ii) perform patching and testing on any cyber equipment, including through the performance of anti-malware and vulnerability scans, in order to identify and correct or mitigate any cyber security weaknesses or vulnerabilities;

2.5 shall ensure that NB Power CEA data possessed by the supplier is properly protected;

2.6 if Contractor is required by NB Power to dispose of NB Power CEAs, it shall ensure that: (i) the disposal is done securely and in a timely manner; and (ii) any associated data is similarly securely deleted;

2.7 shall provide documentation that describes its cyber asset development lifecycle, patch management program, update processes, and cyber security features;

2.8 shall provide updates to remediate any security vulnerabilities in the cyber asset, disclose its mechanisms to deliver updates, ensure its controls will enable NB Power to verify the authenticity and integrity of the updates;

2.9 shall use cyber security best practices in the development of any cyber asset;

2.10 shall comply with all of NB Power's security policies, standards, and procedures as may be provided by NB Power to Contractor from time to time;

2.11 shall ensure that only Contractor's personnel authorized by NB Power are permitted to access, process, store or transfer NB Power CEAs;

2.12 shall ensure that NB Power CEAs are properly protected using appropriate encryption at rest and in transit, and shall use appropriate physical and logical boundary protection in case of processing, storing, or transmitting same;

2.13 shall complete the appropriate tests of the CEA and its critical components in order to provide assurance that all known vulnerabilities are identified and removed, and provide the results of such tests to NB Power;

2.14 shall identify and disable any un-used logical, network-accessible ports and disable any un-used or, any unnecessary physical and logical ports/protocols in the CEA;

2.15 shall ensure it has effective audit and accountability policies and procedures in place that cover cyber security.

NB Power reserves the right to audit Contractor in all aspects of cyber security, including development processes, procedures, practices, and methodologies.

3. CYBER SECURITY DOCUMENTATION and OTHER REQUIREMENTS

Contractor:

3.1 shall draft a compliance letter, which individually lists each of the cyber security items listed in 2. and indicate "Comply" or "Do Not Comply" for each item. A statement should elaborate on "Do Not Comply" items.

3.2 shall package the CEA in sealed, tamper-proof packaging.