CYBER SECURITY PLAN OUTLINE
FOR MODERATE WITH ENHANCED CONTROLS INFORMATION (October 11, 2018)

General Instructions

A Cyber Security Plan (CSP) is required when ORNL *Moderate with Enhanced Controls (MEC)* information will reside on a non-ORNL computer. The CSP is developed to describe the implementation of the required information protection controls. It is developed in the Definition phase of an information system and updated in each phase of the system development.

- At minimum, the CSP must contain the following information for MEC information.
- This plan must be approved by ORNL Cyber Security **PRIOR TO** any MEC information being placed on a non-ORNL computer or other electronic media.
- If the required information is documented in vendor policies or procedures, the CSP should include a reference to those policies/procedures, and a copy should be included as an appendix to the CSP.
- References:
    - Federal Information Processing Standards (FIPS) Publications:
        - FIPS 199: *Standards for Security Requirements for Federal Information and Information Systems*
        - FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*
    - National Institute of Standards and Technology (NIST) Publications:
        - NIST SP 800-53: *Recommended Security Controls for Federal Information Systems and Organizations*
        - NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

1. PROJECT DESCRIPTION AND SYSTEM IDENTIFICATION

1.1. System Name and Identification
1.2. High Level Description of System
1.3. Seller Cyber Security Points of Contact
1.4. Functional Description of System
1.4.1. Information types on the information system
1.4.2. Consequence of loss of confidentiality, integrity, and availability for each information type (reference FIPS 199)
1.4.3. System User Description
1.4.4. Need-to-Know requirements

2. SYSTEM ARCHITECTURE DESCRIPTION

2.1. System Technical Design Description
2.1.1. Hardware
2.1.2. Software
2.2. System Interfaces
2.2.1. Interconnections and External Connections
2.2.2. Memorandums of Agreement (include as appendix in CSP)
2.2.3. System Interconnect Agreements (include as appendix in CSP)

3. ENVIRONMENT DESCRIPTION

3.1. Operating location(s)
3.2. Operating environment

4. SYSTEM SECURITY REQUIREMENTS

4.1.1. NIST SP 800-171 Security and Privacy Controls – Provide documentation addressing each moderate security control in NIST 800-171, in addition to the following NIST 800-53 controls required for MEC information: AC-12 (1), AC-18, CM-2 (1) (2), CM-6 (1), MA-4 (1) (2) (3), MP-3, MP-4, MP-5 (1) (2) (3), MP-6 (1) (2), SC-8 (1), SC-9 (1), and SC-13. Ensure that for each security control Seller policies/procedures are described, along with the specific settings or values including security-relevant settings and policies pushed, if appropriate.

4.2. Data Security Requirements – Include any expanded/increased requirements specified by the data owner/steward.

4.3. Certification of Security Controls Compliance Statement for MEC information – Seller shall provide a written statement of compliance to 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 specified for Moderate information and the additional controls required by ORNL for MEC information – see appendix A.

4.4 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.

Appendix A
Information System Certification

Information System Certification I, the Cognizant Seller Authority, to the best of my knowledge, certify that this Cyber Security Plan contains all the security specifications for operation within 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, in addition to the NIST 800-53 controls required by ORNL for Moderate with Enhanced Controls information. My signature below indicates that I have reviewed this Cyber Security Plan and we will continue to operate to the ORNL standards and to the standards specified herein. Any significant changes to our security posture or implemented security controls will require an update and re-approval of this document.	
Seller's Company Name: _____ Typed Name and Title Cognizant Seller Authority: _____ Typed Name and Title Signature: _____	Date: _____