DISCUSSION DRAFT
CYBERSECURITY REQUIREMENTS

(a) Cybersecurity Risk Management

(1) Definition. "Cybersecurity Risk Management" means technologies, practices, and policies that address threats or vulnerabilities in networks, computers, programs and data, flowing from or enabled by connection to digital infrastructure, information systems, or industrial control systems, including but not limited to, information security, supply chain assurance, information assurance, and hardware and software assurance.

(b) Contract Cybersecurity Risk Management Plan

(1) The contractor shall provide a Contract Cybersecurity Risk Management Plan (CCRMP) containing documentation sufficient to demonstrate its systematic and organizational ability to provide solutions that include appropriate security controls for any task within the scope of the contract. The CCRMP shall also describe how these are related to the organization's enterprise approach to risk management, and how its approach to cybersecurity risk management provides appropriate assurance for the types of deliverables it intends to provide under the contract.

(2) The CCRMP shall be a description of management controls, policies, and processes, and shall not include descriptions of technical security controls. Individual technical security control requirements are not specified in this solicitation. Technical security control requirements will be specified in task order solicitations, based on the cybersecurity risk of the work required by the task order, as determined by the ordering activity.

(3) The CCRMP shall include, at a minimum, a description of:

(i) The management controls, policies, and processes the contractor has in place to address:
(A) Access Control,
(B) Awareness and Training,
(C) Audit and Accountability,
(D) Security Assessment and Authorization,
(E) Configuration Management,
(F) Contingency Planning,
(G) Identification and Authentication,
(H) Incident Response,
(I) Maintenance,
(J) Media Protection,
(K) Physical and Environmental Protection,
(L) Planning,
(M) Personnel Security,
(N) Risk Assessment,
(O) System and Services Acquisition,

(P) System and Communications Protection,
(Q) System and Information Integrity,
(R) Program Management,
(S) Privacy, and
(T) Any other cybersecurity-related management controls, policies, and processes derived from NIST Special Publication 800-53 Revision 4 or other standards or practices that provide equivalent or comparable security.

(ii) Its activities and outcomes related to identification, protection, detection, response and recovery as referenced in the Cybersecurity Framework (http://www.nist.gov/cyberframework) promulgated by the National Institute of Standards and Technology; and

(iii) Its cybersecurity-related activities and outcomes related to Supply Chain Risk Management, including but not limited to what management controls, policies, and processes the contractor requires its subcontractors to have in place to address:
(A) Customs-Trade Partnership Against Terrorism (C-TPAT) Minimum Security Criteria (http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism),
(B) Supplier Risk Management,
(C) Physical security,
(D) Access Controls,
(E) Employee and Supplier Security and Integrity,
(F) Business Partner Security,
(G) Supply Chain Security Training,
(H) Information Systems Security,
(I) Trusted Technology Components,
(J) Secure Transmission and Handling,
(K) Open Source Handling,
(L) Counterfeit Mitigation, and
(M) Malware Detection.

(c) Contract Cybersecurity Risk Management Plan Submittal, Review, and Acceptance

(1) Submittal. All Contract Cybersecurity Risk Management Plans shall be submitted with the proposal. If applicable, the CCRMP shall be appropriately marked as proprietary information. Plans containing confidential business information or proprietary information will be handled according to applicable law and will be used solely for the purposes of managing risk to Government functions.

(d) Contract Cybersecurity Risk Management Plan Update, Review, and Acceptance

(1) Updates.
(i) Annual CCRMP updates are a required deliverable.

(ii) Contractor may update its CCRMP at any other time after contract award to ensure the Government is adequately assured of Contractor's continuous ability to provide appropriate cybersecurity in the deliverables it provides under the contract.

(e) Order Cybersecurity Risk Management Plan (OCRMP) Submittal, Review, and Acceptance

(1) Submittal.
(i) When submitting a proposal in response to any task order solicitation, Contractor shall submit its approved CCRMP to the ordering contracting officer as an addendum to the proposal.
(ii) If required by the task order solicitation, Contractor shall also provide an Order Cybersecurity Risk Management Plan (OCRMP) that includes additional information to address the specific security requirements of the task order solicitation.

(f) Order Cybersecurity Risk Management Plan Update, Review, and Acceptance

(1) Updates.
(i) Contractor may update its OCRMP at any time after order award to ensure the Government is adequately assured of Contractor's continuous ability to provide appropriate cybersecurity in the deliverables it provides under the contract.

(g) Deficiencies

Corrective Action Plan. If any deficiencies are identified during a CCRMP or OCRMP review, the contracting officer shall notify the Contractor of the deficiencies and the Contractor shall submit a corrective action plan to the cognizant contracting officer(s) within [XX] calendar days.

(h) Mitigating Factor.
(1) Contractor's demonstrated compliance with an accepted CCRMP or OCRMP shall be a mitigating factor in determining any remedies the government might pursue against the Contractor in the event of a cybersecurity event or incident which causes damage to the Government.
(2) Contractor has the burden of demonstrating to the satisfaction of the contracting officer, through the provision of adequate evidence, that it was actually in compliance with the accepted CCRMP or OCRMP at the time of the event or incident, and that it has taken appropriate remedial action since the event or incident.

(i) Agency Access. Throughout the term of this contract, and upon 48 hours request, the Contractor shall afford access to all Contractor and Subcontractor facilities, installations, operations, documentation, databases, IT systems, software, hardware,

and devices, and personnel used in performance of the contract, regardless of the location. Access shall be provided to the extent required in the agency's judgment, to assess, validate, and verify Contractor's compliance with an approved CCRMP or OCRMP.