U.S. Department of Education, Office of Chief Information Officer (OCIO) Technical Requirements

1. The contractor shall ensure compliance with Federal and U.S. Department of Education requirements detailed at http://www2.ed.gov/about/offices/list/ocio/legislation.html

2. The Contractor's information systems shall be developed in accordance with the ED Lifecycle Management Framework (LCM), ACS-OCIO 1-106.

3. The Contractor shall ensure that the site complies with OMB Memorandum M-03-22 http://www.usa.gov/webcontent/regs_bestpractices/omb_policies/privacy.shtml which requires the posting of privacy policy.

4. A ".gov" hostname (typically hostname.ed.gov) is required for all government funded websites under OMB Memorandum M-05-04 (http://www.usa.gov/webcontent/regs_bestpractices/omb_policies/domains.shtml).

5. The Contractor shall ensure that all NAGB sponsored content must should be identified prominently with the NAGB logo displayed prominently and links to the ED.gov homepage as appropriate. The compliance policy is described in the http://www2.ed.gov/internal/wwwstds.html#sponsor.

6. The Contractor shall ensure that any non-Federal sponsored websites or content (outside of .gov, .mil, .Fed.us, etc.) that is linked to complies with "ED.gov" Management and Publishing Policies" at http://www2.ed.gov/internal/wwwstds.html#link and the OMB Memorandum http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-04.pdf .

7. The Contractor shall host the website and its associated IT infrastructure within the boundaries and classification level of a pre-existing FISMA certified boundary that has received "Authorized To Operate" status by the U.S. Department of Education or the federal government's FedRAMP program.

8. **Internet Protocol version 6 (IPv6)**: The Contract shall provide COTS solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific criteria to be deemed IPv6 capable are as follows: An IPv6 Capable system must meet the IPv6 base requirements defined by the USGv6 Profile and Testing program at http://w3.antd.nist.gov/usgv6/testing.html. Systems being developed, procured or acquired shall maintain interoperability with IPv4 systems/capabilities. Systems shall

implement IPv4/IPv6dual-stack and shall also be built to determine which protocol layer to use depending on the destination host it is attempting to communicate with or establish a socket with. If either protocol is possible, systems shall employ IPv6. The contractor shall provide IPv6 technical support for system development, implementation and management.

9. IT Systems Security

The contractor, and all sub-contractors, shall comply with the Department of Education's IT security policy requirements, specifically those set forth in the 'Handbook for Information Assurance Security Policy (OCIO-01)', and other applicable procedures and guidance. The contractor, and all sub-contractors, shall develop and implement management, operational and technical security controls to assure required levels of protection for information systems. The contractor, and all sub-contractors, shall further comply with all applicable Federal IT security requirements including, but not limited to, the Federal Information Security Management Act (FISMA) of 2002, Office of Management and Budget (OMB) Circular A-130 Appendix III, Homeland Security Presidential Directives (HSPD), and the National Institute of Standards and Technology (NIST) standards and guidance.

These security requirements include, but are not limited to, the successful Certification and Accreditation (C&A) or Security Authorization (SA) of the system (includes commercially owned and operated systems managed by the commercial vendor and its subcontractors, supporting Department programs, contracts, and projects); obtaining a full Authority to Operate (ATO) before being granted operational status; performance of annual self-assessments of security controls; annual Contingency Plan testing; performance of periodic vulnerability scans; updating all information system security documentation as changes occur; and other continuous monitoring activities, which may include, mapping, penetration and other intrusive scanning. Full and unfettered access for the Department's third party Managed Security Services Provider (MSSP)[1] must be granted to access all computers and networks used for this system. Additionally, when there is a significant change to the system's security posture, the system (Federal and commercial - prime and subcontractors included) must have a new C&A or SA, with all required activities to obtain a new ATO, signed by the Authorizing Official (AO).

System security controls shall be designed and implemented consistent with NIST SP 800-53 Rev 3, 'Recommended Security Controls for Federal Information Systems and Organizations.' All NIST SP 800-53 controls must be tested / assessed no less than every 3 years, according to federal and Department policy. The risk impact level of the system will be determined via the completion of the Department's inventory form and shall meet the accurate depiction of security categorization as outlined in Federal Information Publishing Standards (FIPS) 199, 'Standards for Security Categorization of Federal Information and Information Systems.'

[1] It is incumbent upon all offerors to incorporate anticipated costs into their proposals arising from these activities. Any offeror submitting a proposal inherently accepts the burdens and expenses of these intrusive scans by the Department, third party MSSP vendors, as well as IV&V agents working on behalf of the Department's interests.

System security documentation shall be developed to record and support the implementation of the security controls for the system. This documentation shall be maintained for the life of the system. The contractor, and all sub-contractors, shall review and update the system security documentation at least annually and after significant changes to the system, to ensure the relevance and accurate depiction of the implemented system controls and to reflect changes to the system and its environment of operation. Security documentation must be developed in accordance with the NIST 800 series and Department of Education policy and guidance.

The contractor, and all sub-contractors, shall allow Department employees (or Department designated third party contractors) access to the hosting facility to conduct C&A/SA activities to include control reviews in accordance with NIST SP 800-53, Rev. 3 and NIST SP 800-53A. The contractor, and all sub-contractors, shall be available for interviews and demonstrations of security control compliance to support the C&A/SA process and continuous monitoring of system security. In addition, if the system is rated as 'Moderate' or 'High' for FIPS 199 risk impact, vulnerability scanning and penetration testing shall be performed on the hosting facility and application as part of the C&A/SA process. Appropriate access agreements will be reviewed and signed before any scanning or testing occurs.

Identified deficiencies between required NIST SP 800-53 Rev. 3 controls and the contractor's, and all sub-contractor's implementation, as documented in the Risk Assessment Report, System Security Plan (SSP) and Security Assessment Report (SAR), shall be tracked for mitigation through the development of a Plan of Action and Milestones (POA&M) in accordance with the 'Handbook for Information Assurance Security Policy.' Depending on the severity of the deficiencies, the Department may require remediation before an ATO is issued.

The contractor shall ensure the following:

(a) The IT product/system is monitored during all hours of operations using entrusted detective/preventive systems;
(b) The IT product/system has current antiviral products installed and operational;
(c) The IT product/system is scanned on a reoccurring basis;
(d) Vulnerabilities are remediated in a timely manner on their IT product/system; and
(e) Access/view for cyber security situational awareness on their IT product/system is made available to the Department CIRC (cyber incident response capability).