ATTACHMENT A

Performance Work Statement

Office of Postsecondary Education
01/21/2021

Higher Education Act Title II Accountability

I. AUTHORIZATION

Title II, Sections 205 through 208 of the 2008 amendments to Higher Education Act (HEA) (Title II) requires the 50 states and jurisdictions, the District of Columbia, Puerto Rico and the outlying areas, which include American Samoa, the Federated States of Micronesia, Guam, the Marshall Islands, the Northern Mariana Islands, Palau and the Virgin Islands, to report annually to the Department on the following:

- States' and jurisdictions' requirements and assessments for initial teacher certification or licensure, state teacher standards, criteria for assessing the performance of teacher preparation programs and which programs are under a low-performing or at-risk of low-performing designation, and efforts to improve teacher quality, among others. The state and jurisdiction reports and resources are available at: https://title2.ed.gov/

- Institutions of higher education's (IHE) basic program features, such as admissions requirements, number of students enrolled by gender, ethnicity and race; information about supervision and practice and the number of program completers in traditional and alternative types of programs, pass rates and scale scores on certification or licensure assessments, among others.

Title II also requires the preparation of an annual report based on the annual data collection from the Secretary of Education to Congress and the public on the quality of U.S. teacher preparation and requirements of states' initial teacher certification and licensure. All of the reports submitted through 2016 are available at: http://www2.ed.gov/about/reports/annual/teachprep/index.html
The HEA statute is available at: http://www2.ed.gov/policy/highered/leg/hea08/index.html.

II. PURPOSE

The Office of Postsecondary Education (OPE) in the U.S. Department of Education (Department) is seeking contractual support from an external contractor to:

- Collect and analyze Title II data from states and jurisdictions, IHEs with teacher preparation programs and non-IHE-based programs,
- Develop and maintain the existing database on the quality of U.S. teacher preparation and requirements of states' initial teacher certification and licensure, and

- Update and support the existing website's presentation of Title II data, reports and associated documentation and resources, such as the User Manual and other guidance.

As the public increasingly demands improved schools and increased student achievement, the nation's attention is turned to the role that teacher preparation programs (TPPs) and states have in ensuring that new teachers have the knowledge and skills necessary to help all students achieve academically. In October 2008, Congress again voiced its concern about the quality of teacher preparation by amending Title II of HEA. Additional accountability measures in the form of increased reporting requirements for IHEs, non-IHE-based programs and states on teacher preparation and initial certification and licensing are required.

The data collected supports the Secretary's Title II Report, which is intended to inform Congress, prospective teachers, the education community, IHEs, researchers and policymakers about states' criteria for initial teacher certification or licensure, including criteria for teacher assessment and the quality and features of U.S. TPPs annually. The three-stage web-based reporting process requires IHEs and non-IHE-based programs first report to their states on items related to their TPPs. States then compile a comprehensive report using the IHE and non-IHE-based program data to report to the Department. Lastly, a report based on the state data is submitted to Congress and disseminated to the public. The reporting schedule follows:

- IHEs with teacher preparation programs and non-IHE-based programs report to states by April 30 of each year;
- States and jurisdictions report to the Department by October 31 of the same year, beginning on August 1;
- The Secretary reports to Congress the following April of the following year.

After the report is reviewed and approved by the Department for public dissemination, reports are published on the Web site at: http://www2.ed.gov/about/reports/annual/teachprep/index.html and https://title2.ed.gov/

III. GOVERNMENT FURNISHED INFORMATION

The Government shall furnish the following data/information to the contractor within two weeks from date of award:

1. All necessary Certification and Accreditation information.
2. Contact information for all relevant stakeholders, including IHEs and state and local governments.
3. All data collected under the previous system.
4. System documentation and code for the previous system, including URLs, documentation, data collection system, etc.

IV. TASKS AND DELIVERABLES

The contractor shall complete seven tasks, which are discussed below. All deliverables shall meet the requirements for posting content stated in the ED.gov Management and Publishing http://www.ed.gov/internal/wwwstds.html.

TASK 1: CUSTOMER SERVICE FUNCTIONS

The contractor shall maintain a customer support service system that provides a toll-free telephone "hotline" and email account. The toll-free hotline should be operational on non-holiday weekdays from 8:00 A.M. Eastern Daylight Savings Time to 5:00 P.M. Pacific Daylight Savings Time Monday through Friday. Inquiries shall come primarily from states, and from IHEs, and non-IHE-based programs. It is estimated that state calls occur at more than 50 calls a month during the data collection. While IHEs and non-IHE-based programs report to the state, their calls for technical guidance on the web-based survey are estimated to occur at more than 150 calls per month during data collection. Use of a voice mail messaging system is acceptable for handling calls during peak volume periods, as long as all calls and messages are answered within 24 hours. Inquiries reflect a broad range of topics related to implementation of the HEA Title II data collection, including both technical program questions and operational questions related to reporting and submitting IHE, non-IHE-based, and state data. Inquiries should be resolved, meaning that the customer's question has been fully answered and no further clarification is needed, within 24 hours of initial contact. The customer support service will be the main source of assistance to states, IHEs and non-IHE-based programs as they implement Title II data requirements. Occasionally, inquiries and requests for assistance will be received from Department staff and individuals outside of the Department.

The contractor shall conduct national conference calls with state coordinators, including the insular areas, and TPP representatives on the requirements of the data collection before and during data collection on several dates and times. Eight (8) to ten (10) calls are estimated to be required to service all participants in the data collection. The contractor shall develop a schedule for these calls beginning at least a month in advance of the first call. The contractor shall provide a calling schedule that will be due by December 15 of the base year and all exercised option years. The COR will review the proposed timeline within two weeks of receipt and provide comments. The conference calls will address questions and provide new information on a variety of topics, such as data collection processing updates, system requirement changes, and policy modifications (including changes resulting from reauthorization of the statute) and questions on associated topics. The contractor shall prepare an agenda, develop briefing materials, prepare minutes and summary notes describing the content of the calls, and disseminate materials to participants, as needed. The contractor shall distribute materials two weeks ahead of each call, electronically, in the interest of time and cost.

The contractor shall prepare regular (bi-monthly) and comprehensive Management Information System (MIS) Status Reports on inquirers' issues and/or problems and type of technical assistance provided. The report will state the identity of the caller, number of calls received, answered and unanswered, a description of the topic, progress towards resolution or solution, and

time taken on the call. This report will be provided to the Department on a bi-monthly basis. Ten Ad Hoc reports shall be requested by the COR and through other offices in a contract period.

TASK 2: OUTREACH AND TRAINING SERVICES

The contractor shall provide outreach and training to states, IHEs and non-IHE-based programs using a variety of methods, such as webinars, virtual visits and meetings, and other appropriate formats to states, IHEs, teacher preparation programs, and test companies. The outreach activities will provide training and technical assistance on a variety of topics directed toward improving the quality of the data collection, such as accurate and complete data reporting, validity and reliability of test instruments, reauthorization of the statute, and other customers' needs and questions relating to quality reporting. The contractor shall prepare a schedule/timeline for these activities, including goal-driven draft agendas, dissemination materials, plans for minutes and summary notes listing the participants that will be due within two weeks of date of award for each option year. The COR will review the proposed timeline and activities within two weeks of receipt and provide comments. The contractor shall revise materials within one week of receipt of edits, making the requested changes. The contractor shall disseminate the outreach and training materials one week prior to each activity.

Subtask 2.1: Site Visits

The contractor will virtually visit up to four state agencies or their contracting representatives, including test companies, to resolve complex technical issues. The Department anticipates that virtual assistance to a state or its representatives, testing companies or IHEs or non-IHE-based programs would occur as needed, usually one or two per year. The contractor shall provide documentation outlining issues and a plan to advance problem resolution and find workable outcomes through virtual technical assistance when required.

TASK 3: WEB-BASED DATA COLLECTION SYSTEM AND PUBLIC WEB SITE

Since 2001, OPE has collected data from states on teacher preparation programs, student assessments, and other requirements for initial certification or licensing of teacher candidates. States' standards and policy-related information have also been collected through the web-based Title II data collection system at https://title2.ed.gov.

Title II requires states to oversee the IHE and non-IHE-based alternative route program data collection and serve as their day-to-day contact during their data collection each spring ending on or around April 30. The contractor facilitates the states' data collection process and provides technical support related to the use of the web-based reporting system.

While annual Title II reporting is mandated by statute, the mechanisms IHEs use to report are determined by the state. The Institutional and Program Report Card (IPRC) data entry system is an on-line tool by which IHEs and other organizations with state approved teacher preparation programs can meet the annual reporting requirements on teacher preparation, initial certification and licensing mandated by Title II. If a state chooses to use the IPRC system, all IHEs and non-IHE-based programs in the state must report to the state using this system.

Section 208(c) of HEA, as amended in 2008, mandates that a state is required to provide any and all pertinent education-related information in response to a teacher preparation program's request. Much of the data that the IHEs and non-IHE-based alternative route programs report to their states are also reported to ED. States report their data through a Web-based reporting system called the State Report Card System (SRC).

The Title II Reporting Web Site at https://title2.ed.gov provides information about Title II (Sections 205-208) of HEA. The website includes secure portals for states and institutions with teacher preparation programs to report Title II data. It also provides public access to data about teacher preparation and certification or licensure; technical assistance (TA) materials to support the collection, analysis, and reporting of Title II data; and contact information for the states and testing companies involved in the Title II data collection process. All of the Secretary's Reports to Congress on Teacher Quality and the data supporting them are posted on the website and available to the public.

In addition, the contractor:

- shall develop new public website pages to show new/revised data elements that changed in the 2020 data collections;
- shall maintain tabs/pages that do not require changes in data presentation, or that only require minor tweaks (these may include the Introduction, Providers, and Data Files tabs for each state) so that users may download all the State Report Card data and will present some data displays and maps on data elements that did not change in 2020. This shall include full data displays for all elements of the 2020 State Report Card; and
- shall implement a mobile-friendly version of the reporting system or public website.

Subtask 3.1: Web-based Data Collection System

The contractor shall maintain and operate a Web-based data collection system to collect teacher preparation program information and state requirements for initial certification and licensing data from states as required under Section 205 of Title II. At a minimum, the contractor shall collect the data elements required by the HEA Title II statute, including definitions and summaries as provided in statute or based on the COR's guidance. This may include, with permission of the states, collecting data directly from the testing companies used by the states. The contractor may, with the Department's permission, use contract funds to cover testing companies' data collection costs. The contractor shall pre-populate certain fields (where the required information tends to be stable from year to year) of the data collection system reports for each year using the information provided by the states in the previous year. Title II data collection records have been, and shall, continue to be maintained according to Department records retention requirements (Note to reviewers a copy can be found at: https://connected.ed.gov/Documents/Records Retention and Disposition Schedules.pdf).

The state reports, using IHE and other data, are due to the Department on October 31 of each year**.** However, data collection activities may continue, in a few cases, until November 15. More complete state data may not resolve presenting issues while data checks and quality control features ensure the integrity and quality of the data. Further, at the Department's discretion, data corrections, revisions, and additions may be accepted from states at any point in time prior to publishing the annual report. These edits may result in the rejection of the data or may result in error reports only. The edit checks include both within year and cross-year data file checks.

Annual modifications to the Web data collection system may be required for a variety of reasons, including statutory or policy changes, to improve data quality, or to improve operations and achieve cost efficiencies. Within two weeks of contract award and annually thereafter, the contractor shall prepare an evaluation of all system and process enhancements and improvements (including a timetable and level of effort), based on guidance provided in Task 4, and submit this to the COR for review and approval. System modifications must be fully implemented, tested, and accepted by the COR prior to February 1 for IPRC and August 1 for SRC of each calendar year. All changes and/or enhancements to the data collection system must be approved and accepted by the COR.

The contractor shall ensure that the Web-based data collection system is accessible 98% of the time during the February through April and August through November data collection periods, each calendar year. The contractor shall immediately (within 1 hour of any interrupted service) notify the COR of any interruptions in the data collection and/or Web site services.

During the data collection period, the contractor shall develop and maintain a list of issues related to the electronic data collection processes and system and will propose for the Department's consideration solutions that would enhance and improve the data collection system for the following year. Furthermore, the contractor shall regularly provide reports on the progress of data submissions by states and will notify the Department within 24 hours of any state issues, including information that the state will not be able to meet the reporting requirements or the reporting deadline. The contractor shall work with individual states and their representatives to quickly resolve any system or processing issues and will provide the Department with a summary report. These reports will be provided to the COR at least bi-monthly. At the Department's direction, the contractor shall send email and/or letters to states and their representatives regarding problems with annual data collection.

The contractor shall complete the following:

- Identify system problems.
- Propose solutions.
- Identify options for streamlining collections.
- Identify process and system enhancements or changes to improve the quality, timeliness, and accuracy of the data collection.
- Improve customer services.
- Provide for the cost-effective implementation of policy changes.

COR will review and approve before implementation.

Subtask 3.2: Title II Public Web site

All Title II data and documents are available on the Title II public Web site at https://title2.ed.gov. The website shall be hosted externally by the contractor and must comply with Federal website policies found at https://www.usa.gov/website-policies-and-notices. Additionally, the website must comply with the following information:

- The Web site must have a .gov domain name.
- The Web site must demonstrate affiliation with the Department through some visual means, such as the Department's logo.
- The Web site must display a disclaimer or warning when a user follows a link from a Department website to a non-Government Web site. This disclaimer or warning must state that the site visitors are connecting to is not part of the ED.gov domain.
- The Web site must comply with the Federal Information Security Act of 2002.
- The Web site must have a posted privacy policy – see OMB Memorandum M-03-22.

The contractor shall support and host the Web site, which must meet all the Department's Web standards, including compliance with the requirements of Section 508 of the Rehabilitation Act (See Subtask 4.4). Any publicly available websites (i.e. Subtask 4.1: Web Application – OPE and http://title2.ed.gov/) that result from this effort must include DAP code. Information on implementing DAP code is available at http://www2.ed.gov/web-guidance/stats/dap-code.html. Annually, the contractor shall review the Web site content and format to identify information that is outdated and areas for improvement. The contractor shall propose Web changes to ensure the site is accurate and up to date by June 31. The COR will approve all Web modifications.

Subtask 3.3: Data Analysis and Quality Control

By April 30 each calendar year, the contractor shall have facilitated IHEs and non-IHE-based TPP's reports of Title II information and data to the states. By October 31 of each calendar year, the contractor shall have collected Title II information and data from the states, including data from the IHEs and non-IHE-based programs. At a minimum, the contractor shall collect data elements, definitions and summaries as required by Title II. States are free to include in their reports any additional information they believe would inform the Department and the public about the procedures that they, and IHEs and non-IHE-based TPPs use to prepare their annual reports.

After the annual data collection closes on October 31, the contractor shall review the data collected from the states, IHEs and non-IHE-based TPPs for quality and accuracy. A preliminary data analysis report on the results of quantitative and qualitative analyses, where needed as planned with the COR and program manager, including identifying anomalies or deficiencies is due to the COR within three weeks. The data report shall include computations of the data entry error rate and missing data rate.

The contractor shall prepare the data for states to review, edit in minor ways, complete where required, verify for accuracy and report, which, after corrections, shall be made available to the COR and program manager by January 15.

The contractor shall ensure that access to the data necessary to write the Secretary's report to Congress is provided to the department or contractors working with the department.

Subtask 3.4: Web-Based System Documentation

The contractor shall provide the Department with a system documentation specifying the security components and features that protect the integrity of the data and the system and ensure the reliable availability of information to users. For example, the "user manual" will not contain unnecessary technical jargon and will be available on-line as well as in a printable Word file. The contractor shall assure that security components and features shall protect against external threats and internal vulnerabilities. Security features must consider the operational requirements of an electronic system open to the public, seamless access, which requires consideration of the viruses and back-up. The contractor shall screen for viruses in an environment in which customers are uploading and downloading the Title II files, including graphic files. The contractor shall identify and describe appropriate backup and recovery procedures to restore the system in the event of a virus, crash, or due to other actions or events which lead to corruption of the hardware, software or data files and include this information in the system documentation, which follows:

- System Documentation.
- User Manual.
- Data Dictionary.
- Security Plan.
- Contingency Plan.
- Configuration.
- Management Plan.

The contractor shall provide draft system security documentation in the designated manuals and resources eight weeks after the "kick-off" meeting and, annually by July 15, in exercised option years, specifying the security components and features that protect the integrity of the data, and ensure the availability of information to users for protection against threats, consideration of viruses and describes necessary back-ups and recovery procedures available in the system as described in the subtask. Additionally, the contractor shall update documentation listed below when significant modifications are made to the system. Please see Task 4.0 System Security Administration/Support Application Personnel for additional information.

TASK 4: SYSTEM SECURITY ADMINISTRATOR/ SUPPORT APPLICATION PERSONNEL

The contractor shall support the Title II Web site (title2.ed.gov). The contractor shall maintain a list of proposed and outstanding items for action and will regularly provide updates on implementation/resolution activities bi-monthly. The contractor shall immediately report to the COR after significant changes to the system are made to describe implementations and changes to the security requirements and controls discussed in Task 4 and its subtasks.

Quarterly, the contractor shall review the Web site content and format to identify information that is outdated and recommend areas for improvement. The contractor shall propose Web changes to ensure the site is accurate and up to date. Work performed under this contract must support and comply with the requirements outlined in the following subtasks.

Subtask 4.1: Web Application – OPE

The contractor shall manage and maintain an OPE Web system that is open to public access. When the public accesses an OPE system, OPE must develop and implement security controls to protect the integrity or the application and the confidence of the public. Each OPE Web page must have a designated author or administrator who is responsible for ensuring Web page security and be reported in the System Security Documentation. If a server contains information protected by the Privacy Act, it must not be accessible without proper authorization. Additionally, the Web site should provide notice that it contains Privacy Act information and give notice of the consequences of unauthorized disclosure. Users wishing to access internal OPE systems via the Internet must be authenticated. If ED's security controls are modified, the COR will provide the contractor with the modifications for the OPE Web system.

The Privacy Act Information banner shall contain the following:

> This is a United States Department of Education computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.
>
> This system contains personal information protected under the provisions of the Privacy Act of 1974, 5 U.S.C. § 552a --as amended. Violations of the provisions of the Act may subject the offender to criminal penalties.

The contractor shall be responsible for complying with the requirements of the Privacy Act, 5 U.S.C. 552a, the E-Government Act of 2002, 44 U.S.C. §101, the Federal Information Security Management Act, 44 U.S.C. §3541 (FISMA), as well as OMB directives OMB M-06-16, OMB M-07-16, FIPS 201 and FIPS 140-2. The Contractor shall abide by and follow all Departmental privacy policies, procedures, processes, and standards. All electronically stored sensitive data shall be password protected.

Subtask 4.2: System Login

Login procedures must include an appropriate banner containing the following warning:

> You are about to access a United States government computer network intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.

The banner must include a “click through” requirement so that the person logging in must agree to the terms before accessing the OPE system. Login procedures must also limit the amount of information displayed about the system and its functions until after a user has successfully logged in. OPE systems’ logins must mask a user’s password during login, and must not display the following during login:

- System or application identifiers,
- Help messages, and

- Validation of any portion of the login information, for example, indicating which part of the login data was correct or incorrect.

Subtask 4.3: Passwords

Passwords shall be the access control method used for authentication to an OPE system, the System (Security) Administrator shall document password procedures for each system. The documentation shall include specific information regarding allowable character sets, password length (maximums and minimums), password aging time frames and enforcement approach, and the number of generations of expired passwords disallowed for use. Acceptable OPE passwords must contain a minimum of eight characters in length and include any combination of the following to meet or exceed FIPS Publication 112 standards:

- English uppercase letters (A-Z)
- English lowercase letters (a-z)
- Westernized Arabic numerals (0-9)
- Non-alphanumeric special characters (!, @, #, $, &, *)

Any vender-supplied and/or default passwords on OPE systems must be changed immediately. If users maintain their own passwords, an initial password will be distributed to the user in a secure manner. Immediately upon initial login, users will be forced to change their password. Temporary passwords (if users forget their password) must only be given after positively identifying users. The temporary password must also be distributed to users in a secure manner, and users must change it immediately upon initial login. Users will be informed not to write down or reveal their passwords to anyone. Procedures must be in place for handling lost and/or compromised passwords. Any password transmissions or storage shall be encrypted to prevent capture.

Procedures must be in place describing creation of emergency passwords. These procedures must include who may authorize, duration of password validity, and criteria for granting emergency access. Users must change their passwords at least every ninety days or less if needed. Every system must establish procedures to enforce password changes and identify who changes their passwords.

Subtask 4.4: Systems Security Documentation

In accordance with OMB Memorandum M-05-04, and with the NIST SP 800-44, all publicly accessible Federal websites and web services must have HTTPS enabled, and shall only provide service over a secure connection, and e-mail applications must have SMTP enabled. 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), the National Institute of Standards and Technology (NIST) standards and guidance, and the Federal Risk and Authorization Management Program (FedRAMP) requirements and guidance.

These security requirements include, but are not limited to, the successful Security Authorization (SA) of the system (includes commercially owned and operated systems managed by the commercial vendor and its sub-contractors, 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; revision of 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) 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 sub-contractors included) must have a new 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.'

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 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 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 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 (OCIO-01).' Depending on the severity of the deficiencies, the Department may require remediation before an ATO is issued.

All awarded contracts shall ensure that:

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

Evaluation and Policy Analysis

Internet Protocol version 6 (IPv6)
For IPv6, the contractor 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 like that of IPv4. Specific criteria to be deemed IPv6 capable are:

- An IPv6 capable system that meets the IPv6 base requirements defined by the USGv6 Profile (http://www.antd.nist.gov/usgv6/profile.html).
- Systems being developed, procured, or acquired shall maintain interoperability with IPv4 systems/capabilities.
- Systems shall implement IPv4/IPv6 dual-stack and shall also be built to determine which protocol layer to use depending on the destination host with which it is attempting to communicate or establish a socket. If either protocol is possible, systems shall employ IPv6.

The contractor shall provide IPv6 technical support for system development, implementation, and management.

System Development Standards: Information systems shall be developed in accordance with the ED Lifecycle Management Framework (LCM), ACS-OCIO 1-106.

Reporting of Data Security Breaches

If there is a suspected or known breach/disclosure of PII due to loss, theft, intercepted transfer, or other, the contractor must ensure that this breach is reported to the agency as soon as the contractor has knowledge of it. Per Office of Management and Budget Memorandum M-06-19, Federal agencies have a requirement to report breaches of PII security to a Federal incident response center. OPE must notify the department within 30 minutes of discovering the incident (and the agency should not distinguish between suspected or confirmed breaches). The data security plan must be written to reflect this requirement, and the contractor must provide sufficient notification and documentation of the suspected loss, as it is understood at the time of notification to the agency for this requirement to be met. Follow-up reports of the final status of loss events will also be prepared by the contractor within a reasonable period as advised by the OPE COR.

TASK 5: MEETINGs, CONFERENCE CALLS AND STATUS REPORTS

The contractor shall plan and attend bi-monthly meetings or conference calls, as appropriate, with the OPE Project Manager (or representative), and COR and other Department staff to manage and fulfill the purposes of the project. The contractor shall prepare a monthly status report on activities by task area, which is due by the 10th of each month.

TASK 6: DELIVER REVISED SURVEYS (INSTITUTION AND PROGRAM REPORT CARD [IPRC] AND STATE REPORT CARD [SRC]) FOR SUBMISSION FOR OFFICE OF MANAGEMENT AND BUDGET (OMB) CLEARANCE

Title II is required to collect information from 50 states and jurisdictions, numerous IHEs and non-IHE-based programs in fulfillment of its responsibility to collect data and report on U.S. teacher preparation quality and states' requirements for initial teacher certification or licensure. To do so requires OPE to prepare an OMB package and receive approval to collect program, institutional, and state data in two report cards or surveys. To facilitate the OMB approval process, the contractor shall revise the two surveys, IPRC (https://title2.ed.gov/Public/TA/Reporting_IPRC_2020.pdf) and SRC (https://title2.ed.gov/Public/TA/Reporting_SRC_2020.pdf) to align with Title II required data elements, ensure clear presentation of data elements, provide user-friendly response options, increase efficiency of elements for obtaining complete and accurate data, incorporate feedback from Office of General Counsel, participants in prior collections, expert resources, such as professional associations for teacher preparation and state credentialing, and respond to new regulations or statutory requirements. The surveys shall be prepared by no later than 3 months after start of each period of performance.

TASK 7: TRANSITION AND TRANSFER OF TITLE II RESOURCES (OPTIONAL TASK IN BASE PERIOD AND LAST EXERCISED OPTION PERIOD)

BASE PERIOD:

If a new contractor is selected for this requirement, the new contractor shall meet with the incumbent contractor, Westat, from the previous contract in accordance with Task 8 of Contract EDEPCM16F0001. The new contractor shall work with the incumbent to schedule a meeting(s) to discuss smooth transition of all work and meet the transitional contractual obligations as outlined in the previous contract to minimize a break in services to the greatest extent possible.

LAST EXERCISED OPTION PERIOD:

The contractor shall initiate transitional activities 30 days prior to the expiration of the final exercised option period. The contractor shall provide, no later than the end of the tenth month of the final exercised option period, an electronic document of the contractor's plan for accomplishing transfer of the project should a new contractor be selected. The contractor shall carry out all regular Title II activities without break in services during the transitional phase that include:

- Continued normal services to Title II users for the data collection and website to the last day of the contract.
- As scheduled by the COR, meeting(s) of the current contractor with the new contractor to discuss a smooth transition of all work, and a briefing by the current contractor that provides a detailed discussion of the status of Title II activities and resources.
- Delivery of all Title II databases and documentation, including delivery of complete set of all databases in standard file format with full documentation and delivery of one (1) copy of that set, and its documentation, to the government no later than the last day of the final contract year.
- The transfer of all materials and data information, data, and documentation to an address specified by the Contracting Officer.
- Appropriate close-out of all outstanding financial obligations, technical requirements, and related work.

SCHEDULE OF DELIVERABLES

Higher Education Act Title II Accountability:
The Secretary's Report on Teacher Preparation and State Initial Certification or Licensure

Dates are applicable for base and all option periods.

	HEA Title II Schedule of Deliverables		
No.	**Deliverable**	**Description**	**Date Due***
	Task One: Customer Service Functions		
1.1	Draft National Conference Calls Schedule	Draft a plan a schedule of conference calls with dates and times responsive to time zones for Title II state coordinators and institutions of higher education (IHE) and non-IHE-based teacher preparation programs, including the insular areas, and teacher preparation program representatives on the requirements of the data collection before and during data collection on approximately 8 to 10 occasions.	Draft due to COR December 15 annually or the previous business day if the 15th falls on a weekend.
1.2	Final National Conference Calls Schedule	Provide a finalized schedule of conference calls with dates and times responsive to time zones for Title II state coordinators and institutions of higher education (IHE) and non-IHE-based teacher preparation programs, including the insular areas, and teacher preparation program representatives on the requirements of the data collection before and during data collection on approximately 8 to 10 occasions.	Final due three (3) business days after receipt of COR's two (2) week review comments.
1.3	Draft Conference Call Materials	Draft technical assistance materials, paper and electronic, such as PowerPoints, webinars, etc. to support the calls.	Due to COR three (3) weeks prior to each call.
1.4	Final Conference Call Materials	Final technical assistance materials, paper and electronic, such as PowerPoints, webinars, etc. to support the calls.	Due to COR three (3) business days after COR's five (5) business day review.
1.5	Bi-monthly Status Reports	Status Reports include: • Summaries of Customer Service calls by caller identity, number of calls received, answered and unanswered, a description of the topic, progress towards resolution, and time taken on the call (Task 1). • Briefs of any conferences, webinars, etc.	Bi monthly, on the second and fourth Friday of the month.

		attended on Title II and associated topics (Task 2). • Data Collection Status Reports during data collection cycles (February 1 through April 30 and August 1 through November 30) to include progress of data submissions by states, states needs and impediments, early completers, late starters and the like (Subtask 3.1). • Summary reports of contractor's work with individual states and their representatives to resolve system or processing issues quickly (Subtask 3.1). • List of issues in the electronic data collection processes and system to propose for ED's consideration for enhancing and improving the data collection system for the following year (Subtask 3.1). • Summaries of meetings on management, for workdays, of critical calls to state coordinators, test representatives, etc. (Task 5). • Provide a report of activities by Task Area (Task 5).	
1.6	Ad Hoc Reports	The content and delivery date to be determined (TBD).	Ten reports, dates TBD
Task Two: Outreach and Training Services			
2.0.1	Draft Outreach and Training Schedule	Plan a draft schedule/timeline for outreach and training activities, including goal-driven draft agendas, dissemination materials, plans for minutes and summary notes listing the participants to provide training and technical assistance on a variety of topics directed toward improving the accuracy and completeness of the data collection.	Draft due January 15 annually, or the previous business day if the 15th falls on a weekend.
2.0.2	Final Outreach and Training Schedule	Provide a final copy incorporating the COR's comments on the above document.	Final due one week after receipt of COR's comments from two (2) weeks of review.
2.1.1	Draft Virtual Site Visit Plan	Plan logistics and agenda for virtual site visits to state agencies or their contracting representatives, including test companies, to resolve complex technical issues. Plans	Due within two (2) of identification of issues.

		shall provide documentation outlining issues and a plan to advance problem resolution and find workable outcomes through virtual site technical assistance when required.	
2.2.2	Final Virtual Site Visit Plan	Provide a final version of the above document incorporating the COR's comments.	Due five (5) days after receipt of COR's comments from two (2) weeks of review.
Task Three: Web-based Data Collection System and Public Web Site			
Subtask 3.1: Web-based Data Collection System			
3.1.1	Draft Annual System Modification Proposal	The contractor shall prepare a draft proposal with a timetable and level of effort for all system and process enhancements and improvements, which must comply with the system security requirements outlined in Subtask 4.4.	Proposal due May 30th annually, or the previous business day if the 30th falls on a weekend.
3.1.2	Final Annual System Modification Proposal	A final proposal of the above document incorporating the COR's comments	Due one week after receipt of COR's comments from a two (2) week review period.
Subtask 3.2: Title II Public Web Site			
3.2.1	Draft Web site Review	The contractor shall review the Web site content and format to identify problem areas, needed updates and propose improvements based on current usage and feedback from outreach and training activities. These results shall be formatted as a draft report to the COR.	Annual review due to COR June 30, or the previous business day if the 30th falls on a weekend.
3.2.2	Final Web site review	The contractor shall make modifications based on the COR's comments on the above deliverable.	Due five (5) business days after receipt of COR's comments from a three (3) week review.

Subtask 3.3: Data Analysis and Quality Control			
3.3.1	Data Analyses Report	After the state data collection closes, the contractor shall report on the results of preliminary quantitative and qualitative analysis, including anomalies or deficiencies and include computations of the data entry error rate and missing data rate as described in subtask 3.3.	Data Analysis Report due to COR within three (3) weeks of state collection. closing on October 31st.
3.3.3	State Data Check	After the data collection closes on October 31st, the contractor shall prepare the data for states to review, minor edit, and verify accuracy of their data, which. after corrections, the contractor shall report to the COR and program	Report results of state data check due January 15th after the data collection closes.
Subtask 3.4: Web-based System Documentation			
3.4.1	Draft System Security Documentation	The contractor shall provide draft system security documentation in the designated manuals and resources specifying the security components and features that protect the integrity of the data, ensure the availability of information to users for protection against threats, consideration of viruses and describe necessary back-ups and recovery procedures as required. The contractor shall describe all systems changes and modifications required, and shall incorporate them into the system documentation. See Task 4 for additional guidance on compliance.	Draft system security documentation is due eight (8) weeks after the contract award "kick-off" meeting, and annually, by July 15th in exercised option periods (or the previous business day if the 15th falls on a weekend.)
3.4.2	Final System	The contractor shall provide a final version of the above document incorporating the	Due two (2) weeks after

	Documentation	COR's comments.	receiving edits/changes from the COR after a two (2) week review.
TASK 4: System Security Administrator/Support Application Personnel			
Subtask 4.4: Systems Security Documentation			
4.1.1	Update System Report	Quarterly, the contractor shall review the Web site content and format to identify information that is outdated and recommend areas for improvement. The contractor shall propose Web changes to ensure the site is accurate and up-to-date. Work performed under this contract must support and comply with the requirements outlined in Task 4 subtasks.	Quarterly report due on the last Friday of each quarter (August, November, February, May).
Task 5: Meeting, Conference Calls And Status Reports			
5.1	Submit monthly report of management activities and progress	The contractor will submit a monthly report to describe management activities and progress.	Monthly, by the 10th of each month.
Task 6: Office of Management and Budget (OMB) Information Clearance Package			
6.1.1	Draft Surveys (IPRC and SRC) prepared for OMB clearance	The contractor shall prepare two revised surveys, IPRC and SRC, aligned with Title II required data elements and associated edits to ensure accurate and complete reporting by no later than three months after start of period of performance.	No later than three months after start of period of performance.
6.1.2	Final Surveys prepared for OMB Clearance.	Final OMB package to reflect edits and changes.	Due in five (5) business days after receipt of COR's comments from a three (3) day review period.
6.2.1	Draft Responses to First Federal Register Comment Period	The contractor shall prepare courteous, concise, responsive, and clear answers to every question and comment from the field based on the statute and program requirements and recognize those that are informative and helpful for the program.	TBD.
6.2.2	Final Responses to First Comment Period	Final copy of the above deliverable incorporating COR's comments.	Due within five (5) business days after receipt of COR's comments from a three (3) day review period.

6.3.1	Draft Responses to Second Federal Register Comment Period	The contractor shall prepare courteous, concise, responsive and clear answers to every second-round question and comment from the field based on the statute and program requirements, and recognize those that are informative and helpful for the program.	TBD.
6.3.2	Final Responses to Second Comment Period		Due within five (5) business days after receipt of COR's comments from a three (3) day review period.
Task 7: Preparation for and Implement Transfer of Title II Resources			
7.1	Contractor's Draft Plan for Accomplishing Transfer	The contractor shall initiate transitional activities thirty (30) days prior to the expiration of the contract by describing a plan for carrying out all Title II functions without a break in services during the transitional phase should a new contractor be selected.	Due the end of the tenth 10th month of Option Year Four (or at the end of the last year or performance if all four options are not
7.2	Final Plan for Contractor's Transfer		Due a week after COR's three (3) business day review is received.
7.3	Transfer Certification	The Project Director shall certify that the transfer has been accomplished, and all functions are in place in an email to the COR.	Due three (3) business days before the current contract expires.

*Days refer to business days.

ED IT Security Language for ED IT acquisitions

The contractor shall:

- Complete/update the appropriate level of Security Accreditation (SA) documentation per NIST Risk Management Framework guidance, security controls testing, interagency security agreements (ISAs), and risk assessments in support of government issuance of security assessment and authorization to operate (ATO) decisions

- Ensure that systems/products/applications have the ability to facilitate single-sign-on capabilities and required support for HSPD 12 Personal Identity Verification (PIV) enablement and integration

- Include the capability for network traffic that flows between externally hosted systems and networks, to/from Department systems and networks, to be routed through one of the Department's Trusted Internet Connections (TIC) gateways as part of the solution configuration. Implement controls to ensuring all possible traffic, including mobile and cloud, goes through a TIC. Implement connections between Department systems and networks with externally hosted systems that are in compliance with the requirements of the Trusted Internet Connections (TIC) initiative. https://www.cisa.gov/trusted-internet-connections

- Architect contractor hosting environments to use security isolation and network segmentation principles in order to ensure that the environments are properly protected against an unauthorized access and threat from adversaries who may strive to move laterally across internal Department or contractor hosted systems and network segments.

- Provide an automated capability and process to scan and assess all systems and assets, and associated logs for malicious indicators of compromise (IOCs) identified by the Department regarding priority threat-actor Techniques, Tactics, and Procedures (TTPs); the contractor is required to have the capability to scan for indicators of compromise within 24 hours of receipt of the indicators provided by the Department of Education from the Department of Homeland Security

- Ensure compliance with the 21st Century Integrated Digital Experience Act: https://www.congress.gov/bill/115th-congress/house-bill/5759/text

- Implement and maintain capabilities and processes to support the timely detection of, reporting, and rapid response and recovery to cyber incidents in accordance with timelines and requirements specified in Federal guidance and Department cybersecurity incident reporting policy guidance

- In support of cybersecurity performance measure reporting, the contractor shall implement and maintain an automated software asset management/inventory and hardware asset inventory capability (e.g. scans/device discovery processes) at the enterprise-level.

- Implement capabilities to rapidly deploy emergency security patches and implement specific security control enhancements as directed by the Department of Homeland Security to all Federal Departments via mechanisms such as the DHS Cybersecurity Coordination, Assessment, and Response (C-CAR) action items, and DHS Binding Operational Directives (BODs).

- Implement capabilities and processes to patch all critical vulnerabilities identified to the Department of Education by DHS immediately or, at a minimum, within 30 days of patch release.

- Ensure robust physical and cybersecurity protections are in place for all of the Department's high value assets (HVAs). The identification of HVAs by the Department will be an ongoing activity due to the dynamic nature of cybersecurity risks.

- Implement remote access solutions that only use multi-factor authentication solutions and that prohibit the use of split tunneling and/or dual-connected remote hosts where the connecting device has two active connections.

- Implement remote access solutions that scan for malware before allowing full connections and that time out after 30 minutes (or less) of inactivity and require re-authentication to re-establish a session

- Implement capabilities for all incoming email traffic to pass through anti-phishing and anti-spam filtration at the outermost border mail agent or server

- Implement capabilities for all incoming email traffic to be analyzed using sender authentication protocols (e.g., DKIM, DMARC, VBR, SPF, iprev)

- Implement capabilities that ensure that incoming email traffic is analyzed using a reputation filter (to perform threat assessment of sender)
- Implement capabilities that ensure that incoming email traffic is analyzed for detection of clickable URLs, embedded content, and attachments; and incoming email traffic is first analyzed for suspicious or potentially nefarious attachments and opened in a sandboxed environment or detonation chamber
- Implement capabilities for all outbound communications traffic to be checked at the external boundaries to detect encrypted exfiltration of information (i.e. capability to decrypt/interrogate and re-encrypt)
- Implement effective network segmentation design and security solutions to limit potential threats from adversaries attempting lateral movement across systems on the Department's (or contractor's networks), and also to better protect and securely isolate the Department's HVAs
- Implement and maintain Information Security Continuous Monitoring (ISCM) and Continuous Diagnostics and Mitigation (CDM) capabilities for all IT assets to be subject to an automated inventory, configuration, and vulnerability management capability, with real time reporting
- Implement and maintain strong authentication capabilities requiring the technical enforcement of all users being required to use a Personal Identity Verification (PIV) card to authenticate to the network, (with exceptions for a very limited set of users specifically approved by the Department)
- Develop and maintain (or update existing) System Security Plans (SSP) and security controls assessment (SCA) test plans for the network general support system (GSS), and infrastructure systems
- Provide support to creating the security assessment and authorization (or accreditation) (SA&A) packages and documentation in accordance with the Risk Management Framework guidance and processes specified by NIST and Department guidance
- Implement security configurations on all IT assets and systems using DISA STIGs and other industry recognized best practices or guidance
- Perform security configuration management to include configuring all Windows based systems with the latest United States Government Configuration Baseline (USGCB) security settings available from the NIST website
- Support annual or emergent security audits and security scans that may be performed by the Office of Inspector General (OIG), the General Accountability Office (GAO), or the Department of Homeland Security (DHS)
- The contractor shall provide availability and accessibility to the Department, to the OIG, and to any third party vendors designated by the Department to: 1) Review audit findings; 2) Determine if corrective actions were properly implemented and the associated audit findings were properly closed; 3) Support cybersecurity incident analysis and forensics activities
- Produce scheduled Monthly/Quarterly/Annual security performance measure reports that align to the Department's cybersecurity performance measure reporting requirements specified by OMB for FISMA, the President's cybersecurity Cross Agency Priority (CAP) goals and targets, and CyberScope reporting. Security performance measure reports shall use the format and template specified in the Annual CIO FISMA metrics specified by OMB and DHS.
- Provide for the encryption for PII, CUI, Data at Rest and data in transit, Encryption solutions applied must be FIPS 140-2 validated.

- Document and track contractor personnel cyber training based on roles
- Develop, maintain, and publish a listing of Contractor-provided security controls, hybrid security controls, and "customer"-provided security controls, in support of systems security assessments and authorizations, and the issuance of authority to operate (ATO) decisions by the Department
- Provide security audit support (e.g. A-123), including scheduled and event-driven audits
- Capture and provide forensic disk images to support security incident analysis, malware analysis, or other investigative requirements (such as specific requests from the OIG or law enforcement)
- Provide support for threat monitoring and analysis, incident response, vulnerability management, risk management, continuous monitoring and reporting and other traditional security operations center activities
- Provide and maintain multi-factor authentication solutions utilizing the Personal Identity Verification (PIV) card (or a Department- approved Level of Authentication -4 solution); and utilize FIPS 140-2 approved encryption for all remote access requirements
- Provide robust encryption capabilities to include services such as digitally signed and encrypted email, and default encryption for sensitive information held by the Department. Solutions should be available to enable encryption of as much data at rest and data in transit as possible.
- Identify, perform, track, and report vulnerability and security weakness remediation and mitigation activities through the Department's Plan of Action and Milestones process (POA&M) in accordance with Departmental information security policy
- Establish, maintain, and execute standard configuration management processes for all cybersecurity software and hardware
- Implement and maintain a Privileged Account Management Solution to improve the identity and access management of user accounts, while also meeting Department targets to tightly control and limit the number of users with elevated privileges
- Implement and maintain tightened processes for managing privileged user accounts, to include implementation of capabilities to limit functions that can be performed when using privileged accounts; limit the duration that privileged users can be logged in; limit the privileged functions that can be performed using remote access; prohibit Internet access when privileged users are performing systems administrations tasks; and ensure that privileged user activities are logged and regularly reviewed
- Document and maintain system security boundaries, system configuration details, and network diagrams, in support of security assessment and authorization to operate (ATO) processes
- Develop and implement processes for revising system security documentation on a scheduled and event-driven basis
- Provide support for maintaining system security documentation in support of FISMA reporting requirements and security compliance status in the Department's Cyber Security Assessment and Management (CSAM) system
- Develop and submit system security documentation, risk assessments, security controls testing reports, and any required privacy impact analysis (PIA) to the Department in support of the Risk Management Framework processes and ATO decisions for IT environment components

- Develop corrective/remediation plans of action and milestones (POAMs) and strategies to address security audit and assessment findings, and other reports of system security weaknesses or non-compliance
- Develop and maintain a system security architecture; the contractor's solution shall include effective network segmentation design and solutions to limit lateral movement across systems on the Department's networks, and also better protect the Department's HVAs
- Utilize PIV or other approved Level of Assurance 4, as defined in NIST SP 800-63-2 Electronic Authentication Guidelines, compliant Identity and Access Control mechanisms for network/domain administrative enterprise access.
- Maintain near real-time security monitoring and intrusion detection capabilities to enable the contractor and the Department to know the security risk posture of the network at any given time;
- Configure all Windows based systems with the latest United States Government Configuration Baseline (USGCB) security settings available from the NIST website
- Utilize multi-factor authentication, including integration and compliance with HSPD-12 PIV requirements, for all remote access solutions for the Department's sensitive information systems
- Provide a multi-tier disaster recovery capability that provides the infrastructure and process to meet the recovery requirements of all of its High Value Assets (HVAs), and applications (Mission-Critical, Decision Support, Other)
- Provide IT Disaster Recovery Planning and Management capabilities and support
    - Define business risk and risk assessment
    - Develop disaster recovery strategies
    - Develop disaster recovery plans
    - Develop IT system contingency plans
    - Conduct disaster recovery exercises, training and awareness
- Provide Disaster Recovery Operational Services, including Contractor support to the Department in the planning, preparation, implementation, and documentation of a Disaster Recovery Program that includes the capabilities described below:

The contractor, and all sub-contractors, shall comply with the Department of Education's IT security policy requirements, 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 Modernization Act (FISMA) of 2014, Office of Management and Budget (OMB) Circular A-130, Homeland Security Presidential Directives (HSPD), including HSPD-12, Personal Identity Verification (PIV) Enablement and Integration, and single sign-on, the most recent National Institute of Standards and Technology (NIST) special publications, standards and guidance, and the Federal Risk and Authorization Management Program (FedRAMP) requirements and guidance.

These security requirements include, but are not limited to, the successful Security Assessment and Authorization (SA&A) of the system (includes commercially owned and operated systems managed by the commercial vendor and its sub-contractors, 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 any of the Department's third party Managed Security Services Provider (MSSP) or Cyber-operations prevention testers, or vulnerability scanners, or auditors 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 sub- contractors included) must have a new SA&A, 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 the current, finalized version of the NIST SP 800-53, '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.'

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 SA&A activities to include control reviews in accordance with the current, finalized version of the NIST SP 800-53, and the current, finalized version of the NIST SP 800-53A. The contractor, and all sub-contractors, shall be available for interviews and demonstrations of security control compliance to support the 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 SA&A process. Appropriate access agreements will be reviewed and signed before any scanning or testing occurs.

Identified deficiencies between required security controls within the current, finalized version of the NIST SP 800-53 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 Department policy. Depending on the severity of the deficiencies, the Department may require remediation before an ATO is issued.

The contactor shall provide cybersecurity strategies, infrastructure hosting environments, and solutions that comply with the requirements of the Federal Information Security Modernization Act (FISMA), Department cybersecurity policy guidance, and guidance contained in the NIST Special Publications series such as NIST Special Publication 800-53 and other NIST Special Publications. The contractor shall provide solutions that support the Department's efforts to implement and maintain effective protection activities such as reducing the attack surface and complexity of IT infrastructure; minimizing the use of administrative privileges; utilizing strong authentication credentials; safeguarding data at rest and in-transit; training personnel; ensuring repeatable processes and procedures; adopting innovative and modern technology; ensuring strict domain separation of critical/sensitive information and information systems; implementing network segmentation architectures to better protect and isolate the Department's high value assets and most sensitive information and data; and ensuring a current inventory of hardware and software components. The contractor shall include actions and initiatives to implement the NIST Cybersecurity Framework that emphasizes and measures capabilities to "Identify, Protect, Detect, Respond, and Recover," and ensure that all applicable Service Level Agreements (SLA)s are adhered to, complied with, and satisfied.

All awarded contracts shall ensure that:

1. Their IT product/system is monitored during all hours of operations using entrusted detective/preventive systems;
2. Their IT product/system has current antiviral products installed and operational;
3. Their IT product/system is scanned on a reoccurring basis;
4. Vulnerabilities are remediated in a timely manner on their IT product/system; and
5. Access/view for cyber security situational awareness on their IT product/system is made available to the Department CIRC (cyber incident response capability).
6. All applicable Service Level Agreements (SLA)s are adhered to, complied with, and satisfied.

Internet Protocol version 6 (IPv6)
For IPv6, the contractor 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:

- An IPv6 capable system that meets the IPv6 base requirements defined by the USGv6 Profile (http://www.antd.nist.gov/usgv6/profile.html).
- Systems being developed, procured or acquired shall maintain interoperability with IPv4 systems/capabilities.
- Systems shall implement IPv4/IPv6 dual-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.

Management of Personally Identifiable Information (PII) and / or Sensitive Personally Identifiable Information (SPII):
The contractor shall provide IPv6 technical support for system development, implementation and management.
Per OMB-M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, the following requirements statements should be added to all SOWs/SOOs/PWSs/BPAs/MOUs/IAAs/MOUs/ISAs that include the management of Personally Identifiable Information (PII) and / or Sensitive Personally Identifiable Information (SPII):

- The contractor shall cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- The contractor and subcontractors (at any tier) shall properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies and to comply with any agency-specific policies for protecting PII;
- The contractor shall complete regular Department training for contractors and subcontractors (at any tier) on how to identify and report a breach;
- The contractor and subcontractors (at any tier) shall report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and US-CERT notification guidelines;
- The contractor and subcontractors (at any tier) shall maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity,

determine methods and techniques used to access Federal information, and identify the initial attack vector;

- The contractor shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with this Federal and Department PII Breach Response policies (such as OMB-M-17-12), the Department's breach response plan, and to assist with responding to a breach;
- The contractor shall identify roles and responsibilities, in accordance with Federal and Department PII Breach Response policies (such as OMB-M-17-12), and the agency's breach response plan; and,
- The contractor shall be aware that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

Reporting of Data Security Breaches

If there is a suspected or known breach/disclosure of PII due to lost, theft, intercepted transfer, or other, the contractor must ensure that this breach is reported to the agency as soon as the contractor has knowledge of it. Per Office of Management and Budget Memorandum M-17-12, Federal agencies have a requirement to report breaches of PII security to the United States Computer Emergency Response Team (US-CERT)." The (PO) must notify the department within 30 minutes of discovering the incident (and the agency should not distinguish between suspected or confirmed breaches). The data security plan must be written to reflect this requirement, and the contractor must provide sufficient notification and documentation of the suspected loss, as it is understood at the time of notification to the agency for this requirement to be met. Follow-up reports of the final status of loss events will also be prepared by the contractor within a reasonable period of time as advised by the COR.

Records and Controlled Unclassified Information (CUI)

- "Federal record" as defined in 44 U.S.C. § 3301, includes all information, made or received by a Federal agency in connection with the transaction of public business. ED owns rights to all records produced as part of this contract. Any Contractor rights must be identified as required by FAR 52.227-11 through FAR 52.227-20.
- Federal records must be managed according to the applicable records management laws and regulations, to include the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), 36 CFR Chapter XII Subchapter B, and the Privacy Act of 1974 (5 U.S.C. 552a).
- Federal records which are CUI must additionally be managed in accordance with any applicable laws, regulations and government-wide policies (LRGWP) to include EO 13556, 32 CFR Part 2002, ED Directive OCIO 3-113, and NIST-800-171 Revision 2 (or current version).
- Applicability: This clause applies to all Contractors and sub-contractors (hereafter referred to as "Contractors") and must be incorporated into all subcontracts.
- Training Requirements: All Contractors are required to take the annual Information Management Requirements training. If the contract includes CUI the CUI Identification and Marking Training is required. Additional Category or POC specific trainings may be assigned. Contractor will maintain completion certificates and provide upon request.
- Electronic Information System Requirements: Any electronic information system should address at minimum the following regulations in 36 CFR 1236.10. Agencies must incorporate controls into the system or integrate them into a recordkeeping system that is external to the information system itself (see 36 CFR 1236.20 for recordkeeping system

functionalities). Information systems that process, store, or transmit CUI must fulfill the requirements outlined in 32 CFR 2002.14(g).

- Marking Requirements: The Contractor will mark CUI as outlined in Department training.
- Handling and Safeguarding Requirements: The Contractor will ensure that CUI is managed appropriately. The requirements include safeguarding, controlled environments, shipping and mailing or transporting protections, and reproduction protections (see 32 CFR 2002.14(a-e)).
- Contract Completion Requirements: Removal or destruction of records must be in accordance with assigned ED records schedule and must include written concurrence from the CO/COR. If records are removed or destroyed the Contractor must report the incident to ED immediately. Destruction or removal of records without the above requirements is subject to fines and penalties imposed by 18 U.S.C. 2701.
- Compliance with Information Protection Requirements: ED reserves the right to verify compliance with information security requirements established by this contract. The Contractor will fully comply with all ED-initiated inspections as permissible by law.
- Information Security Incidents (ISI) Requirements: Contractors must immediately report any and all suspected security incidents, breaches, and events involving ED information to ED's Computer Incident Response Center (EDCIRC) and ED's Security Operations Center (EDSOC); EDCIRC@ED.GOV; EDSOC voice: 202-243-6550, regardless of whether the ISI is suspected, known, or determined to involve IT systems operated in support of this contract. In the event of an ISI, ED must be provided immediate access to all IT systems used in support of this contract for inspection and analysis.

IT Accessibility Requirements (Section 508 of the Rehabilitation Act)

- Section 508 of the Rehabilitation Act, as amended by P.L. 105-220, requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Products, platforms and services delivered as part of this work statement that are or contain ICT, must conform to the Revised 508 Standards, at 36 C.F.R. § 1194.1 & Apps. A, C & D.
- Applicable Functional Performance Criteria: When using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards, or when Chapters 4-6 do not address one or more functions of ICT. – All requirements apply
- Applicable requirements for software features and components: All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application – Applies if client server software (installed on a computer) is a part of the procurement.
- Applicable requirements to Webpage and Web Applications: All WCAG Level AA Success Criteria – Applies if websites or a web-based application (browser based) is part of the procurement.

- Applicable requirements for hardware features and components: Applies if hardware is part of the procurement. (e.g. copiers, fax machines, phones, scanner etc.)
- Applicable support services and documentation: All requirements apply.
- Instructions to Offerors: Provide an Accessibility Conformance Report (ACR) for each commercially available ICT item offered through this contract. Create the ACR using the Voluntary Product Accessibility Template. Complete each ACR in accordance with the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanation's column, or through additional narrative.
- Acceptance Criteria: Prior to acceptance, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

SITUATIONAL ED IT Security Language (for specific conditions)

For e-mail:
In accord with BOD-18-01:

- Email Security: Agencies must configure all internet-facing mail servers to offer STARTTLS, and all second-level agency domains to have valid SPF/DMARC records. Additionally, agencies must ensure Secure Sockets Layer (SSL) v2 and SSLv3 are disabled on mail servers, and 3DES and RC4 ciphers are disabled on mail servers:
    - Within one year after issuance of this directive, issued 10-16-2017 (so, due by 10-16-2018), agencies will be required to set a DMARC policy of "reject" for all second-level domains and mail-sending hosts.
    - In accord with OMB Memorandums M-17-06, and M-15-13, and M-08-23, M-10-23, and with Binding Operational Directive (BOD) BOD-18-01, and with the NIST SP 800-52 and with the NIST SP 800-44, all e-mail applications must have SMTP enabled.

For Non-Public Facing Websites:

- Implement capabilities for all inbound network traffic to pass through a web content filter, which provides anti-phishing, anti-malware, and blocking of malicious websites (e.g., fake software updates, fake antivirus offers, and phishing offers)
    - In accord with OMB Memorandums M-17-06, and M-15-13, and M-08-23, M-10-23, and with Binding Operational Directive (BOD) BOD-18-01, and with the NIST SP 800-52 and with the NIST SP 800-44, all Federal websites and web services must be accessible through a secure connection (HTTPS only, with HSTS), and e-mail

applications must have SMTP enabled. The use of HTTPS is encouraged on intranets, but not explicitly required.

- In accord with BOD-18-01: In accord with OMB Memorandum M-08-23, in order to ensure Domain Name System Security (DNSSEC), all federal websites must be hosted on a *.gov location.

For Public-facing websites:

- Implement controls to ensure that all publicly accessible externally hosted Department websites and web services only provide service through a secure connection, (such as the Hypertext Transfer Protocol Secure (HTTPS)).
- Implement controls to ensure that all publicly accessible Department websites and web services only provide service through a secure connection, (such as the Hypertext Transfer Protocol Secure (HTTPS))