



## Office of Inspector General Technology Contracts

**Report C-2021DOE-008**

**June 2021**

---

### Executive Summary

In accordance with the Department of Education's (department) fiscal year 2020-2021 audit plan, the Office of Inspector General conducted a consulting engagement of the department's technology contracts or agreements. The purpose of this engagement was to determine whether technology contracts conform to enterprise standards, applicable frameworks, and legal and regulatory requirements and effectively manage risk related to the provision of Information Technology (IT) services.

During this engagement, we noted that, in general, the department's technology contracts appropriately addressed security and risk management requirements. Through this engagement, we identified potential areas of improvement for the department's technology contract templates related to the retrieval of proprietary data, the destruction of data at contract termination, and conducting background screenings before the department enters into business with a contractor or vendor.

---

### Scope, Objectives, and Methodology

The scope of the engagement included an examination of a sample of department technology contracts and agreements to acquire or maintain information technology (IT) systems from July 1, 2019, through the end of fieldwork. The objective of this engagement was to determine whether the technology contracts or agreements conformed to enterprise standards, applicable frameworks, and legal and regulatory requirements and effectively managed risk related to the provision of IT services.

To accomplish our objectives, we reviewed applicable laws, rules, and regulations; reviewed enterprise standards and applicable frameworks; interviewed appropriate staff; reviewed contract templates; and reviewed a sample of executed technology contracts or agreements and related documents.

---

### Background

The Bureau of Contracts, Grants, and Procurement Management Services provides multiple specialized services for the department, managed by its individual offices.

The Office of Contracts and Procurement manages the processes for executing, amending, and monitoring implementation of contracts on behalf of the department. This office also is responsible for implementing all purchases for the department in accordance with state and federal laws and rules, thus assuring that goods and services are procured at the best value for the state. The Office of Grants Management oversees all aspects of grants management, grant training, and grant development for state and federal grants and sub-grants.

The Procurement Office provides expertise in the procurement of products and services to department staff ensuring procurement activities are performed within law, rule, policy and procedure. The Contract Office is responsible for administering the department's contracting activities for commodities and services in accordance with Section 287, Florida Statutes (F.S.) and Chapter 60A-1, Florida Administrative Code (F.A.C.). The Contract Office ensures that the department, through its contracting process, protects the funds it disburses; obtains maximum services for the dollars spent; and complies with applicable state, federal, and departmental laws, rules, and regulations governing contract procurement and contract management activities.<sup>1</sup>

The Division of Technology and Innovation (DTI) is responsible for Technology Planning and Management; Educational Technology; Data Center Operations; Applications Development and Support; and Customer/End User Support. Since July 2020, DTI has assumed contract management responsibilities for the Division of Vocational Rehabilitation (DVR) and the Division of Blind Services (DBS) staff augmentation and information technology (IT) contracts.

We requested all current department technology contracts from DTI, DVR, and DBS. DVR did not have any active technology contracts during the scope of the engagement. We selected four IT contracts or agreements for review. The contracts or agreements selected include: Alliance-Aware software, Florida Safe Schools Assessment Tool (FSSAT), Northwest Regional Data Center (NWRDC), and CPALMS (Collaborate, Plan, Align, Learn, Motivate, Share) and Student Tutorials. (Note: CPALMS is a project award.)

## Consulting Results

---

The consulting engagement focused on the inclusion of Information Security and Risk Management provisions in the department's standard contract template as well as the four selected information technology (IT) contracts or agreements. We determined that the sampled department technology contracts follow the standard department contract template.

The contract template is broken up into five sections:

- Attachment A: Detailed Description of Performance Duties
- Attachment B: Payment Terms and Schedule
- Attachment C: Standard Terms and Conditions
- Attachment D: Audit Requirements
- Attachment E: Minority Subcontractors Utilization Summary

---

<sup>1</sup> <http://www.fldoe.org/finance/contracts-grants-procurement/>

We reviewed information security language including the confidentiality of data, breaches, change control, and background screenings. We additionally reviewed the contract templates and selected IT contracts and agreements to determine whether they included the appropriate risk management requirements, language regarding the management and ownership of data, and language detailing what occurs when service is not fully rendered. Upon review of the contract templates and sampled IT contracts and agreements, we identified areas of improvement in the areas of background screenings, retrieval of data, and destruction of data. See details below.

#### Background Screening Language

Upon review of the department's contract template, we determined the template does not clearly state that a background screening must be conducted prior to any contractor accessing the department's environment.

Per Attachment C, section XXXII (32), of the contract template, "A person or affiliate who has been placed on the convicted vendor list following a conviction for a public entity crime may not submit a bid on a contract to provide any goods or services to a public entity, may not submit a bid on a contract with a public entity for the construction or repair of a public building or public work, may not submit bids on leases of real property to a public entity, may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity, and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017, F.S., for CATEGORY TWO for a period of thirty-six (36) months from the date of being placed on the convicted vendor list."

Section XXXVII (37) of the template also states, "Contractors, providers, and partners employed by the Department or acting on behalf of the Department shall comply with Florida Administrative Code (F.A.C.) 74.2, and fully comply with all information technology security policies. Contractors, providers, and partners employed by the Department or acting on behalf of the Department shall also fully comply with 60GG-2 Information Technology Standards." Per F.A.C. 74-2.002 (1)(f)(9) and 60GG-2, it is the responsibility of each agency to "perform background checks and ensuring that a background investigation is performed on all individuals hired as IT workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher". Due to these positions normally having privileged access, in addition to the agency required background check, a federal criminal history check must be conducted in tandem.

Upon review of each sampled contract's security language, we determined all four contracts included the Attachment C language noted above. However, three of the four sampled contracts or agreements did not clearly state that a background check must be conducted prior to a contractor accessing the department's environment. The Florida Safe Schools Assessment Tool (FSSAT) contract was the only sampled contract that included specific language regarding background screenings. Per the contract, "The Contractor shall be required to submit a resume and Level II background screening to the Department for all Information Technology staff augmentation employees. Such employees shall be approved by the Department in writing prior to such employee beginning work on this contract." We noted this language differs from the F.A.C. 74-2 and 60GG-2 requirements for the agency to conduct background checks on individuals hired as IT

workers. It additionally does not include a requirement that the background checks screen for felony convictions for the following crimes as identified in the F.A.C. 74-2 and 60GG-2:

- a. Computer related IT crimes;
- b. Identity Theft crimes;
- c. Financially-related crimes, such as; fraudulent practices, false pretenses and fraud, credit card crimes;
- d. Forgery and counterfeiting;
- e. Violations involving checks and drafts;
- f. Misuse of medical or personnel records; and,
- g. Theft.

Lack of contract language specifying the requirement for all contractors and vendors to undergo a background screening prior to accessing the department's IT environment could expose the department's confidential data to unnecessary risk. By not specifying this requirement, the department risks entering into business with entities that may not appear on the convicted vendors list but employs individuals with criminal records who should not have access to confidential information.

Recommendation:

We recommend the department add a section to the contract template and applicable procurement instrument that specifically states background checks should occur prior to the contractors or vendors beginning work if the contractor or vendor will have access to department IT environments. We recommend that the department establish policies and procedures related to background screenings, which include the identification of disqualifying criteria for individuals who will have access to the department's environment.

Data Retrieval and Disposal

We reviewed the contract template to identify language regarding the management and ownership of data and how that data will be retrieved in the event that a contract expires or is voided. The contract template includes Section XII (12) which details the circumstances for which intellectual property will be solely owned by the State of Florida. F.A.C. 74-2.003(4) (c) includes the necessary procedures for sanitization of any media device that may contain confidential or exempt information. The information must be rendered unusable, unreadable, indecipherable, and unable to be retrieved or reconstructed. This section also requires the documentation of the procedures taken for sanitization whether it be done via software to overwrite data on computer media, degaussing, or physically destroying media. However, neither Section XII (12) nor the F.A.C clearly addresses how data should be retrieved or destroyed at the conclusion of the contract.

Upon review of the sampled contract's security language, we determined that three of the four contracts do not clearly state how data will be retrieved from the contractor or vendor at the conclusion of the agreement. The exception was the NWRDC service agreement. Both the department and NWRDC hold their own disaster recovery plans that include information regarding the retrieval of data. We additionally noted that the sampled contracts contain language that requires the department to destroy the vendor's data and return licensed software; however, the contracts do not stipulate that the vendor or contractor should destroy the

department's data upon conclusion of the agreements. For example, Section 7(c) Effect of Termination of the Alliance-Aware software contract requires the licensee (the department) to "immediately cease all use of the Aware software, the associated User documentation and Technical Documentation in whatever form or media embodied, and any other materials related to Aware Software, destroy all such software and materials if they exist in electronic form or, alternatively, return them to Alliance; certify in writing that no copies thereof remain in Licensee's possession or under its control." There is no such clause regarding any department data that may be in the possession of the contractor.

Lack of contract language specifying how data is retrieved upon conclusion of an agreement could result in the department being unable to retrieve usable data upon the conclusion of the contract. This could lead to the loss of mission critical data and possible monetary damages. In addition, lack of contract language specifying when and how data is to be disposed upon the conclusion of a contract, or when the data is no longer useful, could lead to potential breaches or the inadvertent release of confidential information. Though our contract template states that the department will be the sole owner of anything produced as a result of any contract, the inability to retrieve critical data stored in a proprietary system could adversely affect business continuity.

Recommendation:

Since the contract template is used department-wide and not every contract will include IT requirements, we recommend a placeholder be added to the template and applicable procurement instrument regarding the ownership and retrieval of data. The placeholder could include a requirement that the vendor or contractor provide a digital, reusable copy of the data, in whole and in parts, as a platform independent and machine-readable file. A reusable copy should be made available in a well-documented and non-proprietary format, with a clearly-defined data structure and a data dictionary for all terms contained in the data.

We also recommend the department add a placeholder to the contract template related to the destruction of data upon the conclusion of the contract or when there is no longer a need to store the data. The language should ensure that department data stored by the contractor is sanitized and rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction.

Lastly, we recommend that, following the termination of any contract in accordance with the provisions of said contract, the department require the contractor to:

- a. Return promptly to the department all physical copies of confidential data in the contractor's possession or in the possession of its representatives; and
- b. Destroy all electronic copies of such confidential data, information, and notes including electronic copies prepared by the contractor or any of its representatives, in a manner that ensures the same may not be retrieved or undeleted.

Alternatively, we recommend the department consider creating and implementing a contract template specific to IT which contains the recommendations above and conforms to enterprise

standards, applicable frameworks, legal and regulatory requirements, and effectively manages risk related to the provision of IT services.

### Closing Comments

---

The Office of the Inspector General would like to recognize and acknowledge the Division of Technology and Innovation and staff as well as the Office of Contracts and Procurement for their assistance during the course of this engagement. Our fieldwork was facilitated by the cooperation and assistance extended by all personnel involved.

*To promote accountability, integrity, and efficiency in state government, the OIG completes audits and reviews of agency programs, activities, and functions. Our audit was conducted under the authority of section 20.055, F.S., and in accordance with the International Standards for the Professional Practice of Internal Auditing, published by the Institute of Internal Auditors, and Principles and Standards for Offices of Inspector General, published by the Association of Inspectors General. The consulting engagement was conducted by Elie Emile and supervised by Tiffany Hurst, CIA, Deputy Inspector General.*

*Please address inquiries regarding this report to the OIG's Audit Director by telephone at 850-245-0403. Copies of final reports may be viewed and downloaded via the internet at <http://www.fldoe.org/about-us/office-of-the-inspector-general/audit-reporting-products.stml>. Copies may also be requested by telephone at 850-245-0403, by fax at 850-245-9419, and in person or by mail at the Department of Education, Office of the Inspector General, 325 West Gaines Street, Suite 1201, Tallahassee, FL 32399.*