# Exhibit F

## Additional Contract Language for American Rescue Plan Act (ARPA) Emergency Solicitation: Child Care Grant Management Solution

Unless otherwise agreed to by the OCFS in writing, the contractor's current version of the software application must function as specified in the associated SoW in an environment comprised solely of components including, but not limited to operating system and database platform versions which are in an active support phase (e.g., no requirement to run on EOL life software such as Windows 7, etc.)

The Contractor shall represent the below practices by providing the documentation of Contractor's adherence to the below policies available in a public website or secure portal that shall be provided to OCFS upon request.

Secure System Development Lifecycle

Policies that govern software development practices commensurate with the risk of the intended use of each software application

a. Such policies shall define documented security roles for the software development team
b. On no less than an annual basis, the contractor shall conduct a comprehensive review of software development policies and make changes where indicated to adequately address new or changed risk

At least annually, the contractor shall provide training in secure software development practices to its developer workforce.

a. Such training shall be focused on the technologies in use within the software development environment
b. Such training shall include a review of the contractor's chosen secure coding framework (see "Vulnerability Management" section) and related policies, procedures and standards
c. Such training shall include a review of the security-related roles and responsibilities conferred on development personnel by organizational policy

The contractor shall, to the extent legally permissible, conduct criminal background checks, credit checks and reference checks for all personnel engaged in the software development process, and establish a set of criteria for when management must be engaged regarding the results of such checks.

The contractor shall deliver remote and /or on premises support only with approval of OCFS and with the option for OCFS to supervise / observe the support activity

At no time during remote and /or on premises support, or any other time, shall contractor transfer OCFSs data from OCFS's on premise installation of the software application to a remote location without the express written permission of OCFS

The contractor shall:

1. utilize uniquely assigned credentials for each of its workforce members to be used in supporting OCFS's software application and

2. notify OCFS within 24 hours of the departure of a contractor's workforce member who had knowledge of credentials used to support the OCFS's software application, if those credentials are on a NYS supported system

Upon request and with reasonable notice, the contractor shall provide OCFS with a list of its workforce members with knowledge of credentials used to access OCFS's software application.

The contractor shall implement hashing within its artifact repositories along with automated controls to ensure that releases are built only from approved artifacts.

For software applications deemed mission critical by OCFS, the contractor shall maintain ISO27001 (27034), ISO9001 (90003) or BSA Framework for Secure Software compliance, or compliance with a similar framework mutually agreed with OCFS.

The contractor shall establish a core set of security requirements to be used in the acquisition of commercial and open source components for the software development environment and software applications developed therein.

The contractor shall develop code within an Integrated Development Environment application with built in error / security checking enabled.

The contractor shall store all source and compiled code in code repositories with access limited to authorized personnel based on role.

The contractor shall maintain separate environments for development and testing

The contractor shall perform adequate testing on software applications used by OCFS including, but not limited to security testing, unit testing, integration testing, regression testing, load testing, and user acceptance testing.

The contractor shall not perform application testing with un-sanitized customer data without the express written permission of OCFS.

The contractor shall implement access management controls such that all access to the software development environment by the workforce is made via uniquely assigned accounts.

The contractor shall aggregate, protect and analyze all logs generated by systems involved in the software development process.

The contractor shall implement multifactor authentication for sensitive functions within the software development environment, as well as for all access to the software development environment from outside the contractor organization.

The contractor shall adequately protect the development environment from the rest of its business environment through strategies such as network-layer segmentation, and the use of endpoint protection software and host-based firewalls on all development endpoints.

The contractor shall utilize one or both of the following methods to ensure that no single workforce member can implement an unauthorized change to the software application:

a. Technically enforced separation of duties such that workforce members who write code may not compile code into a releasable software application
b. Automation maintained within the software development environment which ensures that peer security code reviews are performed prior to commits to a source code repository, along with supporting controls to ensure that releases are built only from approved repositories that are not accessible to development personnel

The contractor shall provide a "Software Bill of Materials" to OCFS detailing all third party components included in the software. This SBOM shall be provided upon initial contracting and any material change to the components of the software thereafter the contractor's current version of the software application must function as specified in the associated SoW in an environment comprised solely of components including, but not limited to operating system and database platform versions which are in an active support phase (e.g., no Windows 7 requirement, etc.).

Client installations of software applications intended for end users (i.e., not IT administrative applications), must deliver the functionality as specified in the associated SoW solely with "user-level" permissions, and not require "root-level" or "administrator-level" permissions for the end user.

The contractor or a qualified third party (this could be ITS but will require at minimum 1 week lead time, depending on application size) shall conduct vulnerability scanning against each proposed release of the Software. The contractor shall implement dynamic and static analysis in the software development environment to identify vulnerabilities.

The contractor shall, on at least an annual basis and upon substantive change in software application features or functionality, engage a qualified third party (this could be ITS but will require at minimum 2 weeks lead time, depending on resource availability, application size and scope) to perform an application penetration test against the software application.

The contractor shall provide the Executive Summary, including number of vulnerabilities and associated severity, from its most recent vulnerability scan and penetration test performed against the software application prior to the software going live.

The contractor shall notify OCFS via mutually agreed methods and within no more than 24 hours of any vulnerability identified within its released code with a CVSS version 3 severity of 4.0 or higher.

The contractor shall make commercially reasonable efforts to ensure that components including but not limited to third party libraries, components and APIs are maintained at their most recent, stable version within the released application made available to OCFS.

The contractor shall follow a secure coding framework appropriate to the nature of its software application. For example, web application development teams may follow the Open Web Application Security Project's Secure Coding Practices.

The contractor shall document and execute a remediation plan for any vulnerability identified through dynamic or static analysis, vulnerability scans or penetration tests.

The contractor shall establish processes for monitoring and acting upon vulnerability notices published regarding components of the software development environment as well as components used in the software application provided to OCFS.

The contractor shall maintain publicly available mechanisms for receiving reports of vulnerabilities identified by its customers, security researchers and similar entities.

The contractor shall ensure that any open source licenses which apply to components used in the software application confer no obligations upon OCFS, or that in the event of such obligation, OCFS is aware of and agrees to same.

All applications released by contractor to OCFS shall be signed by a publicly trusted code signing certificate so that OCFS may verify the authenticity and integrity of the release. This code signing certificate shall be rotated on at least an annual basis.

The contractor shall ensure that all implementation services and / or guides comprehensively address security hardening for the application. Such hardening shall include, but not be limited to, the disabling of unnecessary features based on the SoW and the implementation of a "least privilege" access model for all users and service accounts.

The contractor shall implement processes to ensure that all changes to the software application:

a. Are made at the direction of its product managers or equivalent role
b. Are documented in a work management / issue tracking application
c. Maintain evidence of security checks and approvals
d. Include documented functional requirements and non-functional security requirements
e. Include a plan for notifying customers, including OCFS, of any substantive changes upon release

The contractor shall provide ample notice, and in no case less than six months, should the software application or application version used by OCFS reach End of Life, such that it will no longer receive security updates to address vulnerabilities.

The contractor shall implement processes to identify and respond to any unauthorized changes in the software development environment, including but not limited to source code and artifact repositories, access management controls, etc.

The contractor shall monitor the support status of all components of the software development environment, maintaining them at a supported level.