State of Iowa FY2021 Amendment to
The Drupal Managed Services Contract #2017BUS601

This FY2020 amendment (the **"Amendment"**) amends the **Drupal Managed Services Contract #2017BUS601** (the **"Agreement"**) dated June 6th, 2017 between the State of Iowa, by and through the Office of the Chief Information Officer (**"OCIO"**) and Webspec Design, LLC (**"Contractor"**), to include the FY2020 Standard Requirements as further defined in Section A, and the FY2020 Strategic Requirements, as further defined in Section B.

To the extent of any conflict or inconsistency between the specific provisions of this Amendment and the Agreement, the terms of this Amendment shall prevail. The parties may be referred to herein individually as a **"Party"** or collectively as the **"Parties."** Notwithstanding anything in this Amendment or Agreement to the contrary, individual Purchasing Instruments executed by or individual purchases otherwise made by Governmental Entities shall be deemed to incorporate the terms and conditions of this Amendment and shall constitute a separate, distinct and independent agreement between the applicable Governmental Entity and Contractor, and such Governmental Entity shall be solely responsible for any payments due and duties and obligations owed under this Amendment and any Agreement.

A. FY2021 Standard Requirements

OCIO requires certain tasks to be completed in order to ensure consistency between all citizen-facing State of Iowa websites. Tasks identified herein will be completed by Webspec Design, LLC ("Contractor") on an as needed basis, as determined by Contractor, and will be billed to Agencies consistent with the Drupal Managed Services Contract #2017-BUS-601 (the "Agreement"), RFP1216185012, and the Agency SOW. Citizen-Facing Website Requirements include the following tasks:

1. **Service Request Tracking**
   Contractor will use State-approved ticketing system as directed by the State of Iowa to manage all work associated with these Requirements including intake of maintenance and operation requests, incidents, and change management.
   - 1.1. Contractor will use State-approved ticketing system to track and resolve incidents. An incident ticket indicates that something is broken on the website or that the website is down.
   - 1.2. Contractor will use State-approved ticketing system to record and manage work for all requests. A request is a new site or an enhancement to the existing site and includes requests for assistance with Google Search, Google Analytics, and user access.
   - 1.3. Contractor will use State-approved ticketing system to track all changes related to Drupal, Apache, MySQL, MariaDB, and PHP as noted in Sections 2 and 3.

2. **Security**
   Contractor will ensure that all components above the operating system, including the HTTP server, PHP, database server, and Drupal Core, are managed in a way that maximizes confidentiality, integrity, and availability. Actions will include but are not limited to the following:
   - 2.1. Contractor will track, test, and remediate all security threats.
   - 2.2. Contractor will test, deploy, and apply Drupal Core, Drupal Contributed Projects releases, and Public Service Announcements fixing vulnerabilities receiving a security risk level designation of Critical or above immediately upon availability without agency prior approval. "Critical" is defined at https://www.drupal.org/security-team/risk-levels.
   - 2.3. Contractor will test, deploy, and apply Drupal Core, Drupal Contributed Projects releases, and Public Service Announcements fixing vulnerabilities receiving a security risk level designation of

Moderately Critical or below with agency prior approval. “Moderately Critical,” “Less Critical,” and “Not Critical” are defined at https://www.drupal.org/security-team/risk-levels.

2.4. Contractor will test, deploy, and apply Apache releases fixing vulnerabilities rated with a Critical impact immediately upon availability without agency prior approval. “Critical” is defined at https://httpd.apache.org/security/impact_levels.html.

2.5. Contractor will test, deploy, and apply Apache releases fixing vulnerabilities rated below Critical impact with agency prior approval. “Important,” “Moderate,” and “Low,” are defined at https://httpd.apache.org/security/impact_levels.html.

2.6. Contractor will test, deploy, and apply MySQL releases fixing vulnerabilities rated with a Critical (S1) impact immediately upon availability without agency prior approval. “Critical (S1)” is as defined at https://bugs.mysql.com/.

2.7. Contractor will test, deploy, and apply MySQL releases fixing vulnerabilities rated below Serious (S2, S3, S4, or S5) impact with agency prior approval. “Serious (S2),” “Non-Critical (S3),” “Feature Request (S4),” and “Performance (S5),” are as defined at https://bugs.mysql.com/.

2.8. Contractor will test, deploy, and apply MariaDB releases fixing vulnerabilities rated “red” immediately upon availability without agency prior approval. “Red” is as defined at https://mariadb.org/about/security-policy/.

2.9. Contractor will test, deploy, and apply MariaDB releases fixing vulnerabilities rated “yellow” with agency prior approval. “Yellow” is defined at https://mariadb.org/about/security-policy/.

2.10. Contractor will test, deploy, and apply PHP releases fixing security issues rated at High Severity immediately upon availability without agency prior approval. “High Severity” is as defined at https://wiki.php.net/security.

2.11. Contractor will test, deploy, and apply PHP releases fixing security issues rated at Medium Severity or Low Severity with agency prior approval. “Medium Severity,” and “Low Severity,” are as defined at https://wiki.php.net/security.

2.12. Contractor may otherwise mitigate the effects of known vulnerabilities by implementing adequate compensating controls in the event of the occurrence of Drupal, Apache, MySQL or MariaDB, or PHP vulnerabilities for which a security patch cannot immediately be deployed for cognizable technical justifications.

2.13. Contractor will notify agency and OCIO of any mitigating act implemented pursuant to section 2.12, and include with their notification an explanation and justification for use of the mitigating act.

2.14. Contractor will notify agency and OCIO in the event of the occurrence of Drupal, Apache, MySQL, or PHP vulnerabilities for which a security patch requires agency approval, and the agency does not timely provide approval. Notification of the non-consent will include an explanation of the circumstances surrounding the non-consent.

2.15. Contractor will give the agency the opportunity to pre-approve all updates and patches, waiving the prior approval requirement per update or patch described in 2.3, 2.5 2.7, 2.9, and 2.11. Contractor will provide notification to agencies when the update or patch is moving into production.

2.16. Contractor will only use stable releases of Drupal modules on production State of Iowa websites. Alpha, Beta, or release candidate modules will not be used.

2.17. Contractor will ensure all standard and custom Drupal modules are updated on a routine basis as agreed to with agency and OCIO. Contractor will put the update into test for agency to conduct User Acceptance Testing and if it passes, implement it in production at no additional cost; if the module doesn’t pass, then the contractor will provide to the customer an estimate of costs to remediate issues to conclude UAT and implement in production.

2.18. Contractor will complete an OCIO approved security scan for all new code packages and existing

custom code packages. New code packages include, but not limited to, Drupal websites and new Drupal modules. New code packages must pass the OCIO approved security scan before being deployed to production. Existing custom code packages include, but not limited to, the Iowa Web Design System (IAWDS) used for creating new sites. Contractor agrees to remediate issues in the IAWDS as identified by security scans and receives approval from OCIO.

2.19. Contractor will submit to routine examination of the code. Contractor will notify OCIO/AppDev when code involves sensitive information. When new code packages involve sensitive information, OCIO will conduct a code review for first time code deployments and subsequent updates to code to ensure the contractor adheres to OCIO standards and industry best practices for protecting sensitive information.

2.20. Contractor will ensure all websites function behind State-approved website protection tools required by the State of Iowa.

2.21. Contractor will submit to routine examination of the database server software configurations, ensure adequate logging and monitoring in conformance with OCIO requirements, and generally conform to guidance provided by the OCIO concerning secure and optimal configurations of all components supporting Drupal.

2.22. Contractor will provide the OCIO Information Security Division with a list of all citizen-facing State of Iowa websites maintained by the contractor.

2.23. Contractor will report security incidents involving citizen-facing State of Iowa websites to the OCIO Information Security Division soc@iowa.gov.

2.24. Contractor will ensure Drupal sites log developer and administrator access to the site.

2.25. Contractor will not use shared developer/administrator accounts to access Drupal sites.

3. **Operational Management (Front end)**

3.1. Contractor will optimize the Iowa Google Custom Search Engine so that Agency web pages have priority returns over non-agency pages within all *.iowa.gov pages. Contractor will provide support for Google Custom Search engine including assistance with requesting access and initiating accounts. Contractor will provide basic guidance on the training website mentioned in section 5.5.

3.2. Contractor will provide support for Google Analytics. Support will include configuring each agency website with a Google Analytics tracking code and replacement of codes where necessary.

3.3. Contractor will provide guidance and support to keep websites in compliance with Section 508 of the Rehabilitation Act of 1973 as amended.

3.4. Contractor will implement module updates and enhancements across all applicable agencies to standardize agency consistency and uniformity whenever possible.

3.5. Contractor will work with OCIO to develop and implement a web site backup and recovery plan that addresses all requirements of the OCIO hosting environment.

3.6. Contractor will test the backup and recovery plan quarterly by the Contractor. Quarterly backup and recovery plan test results will be provided to agency and OCIO in the Quarterly Master and Agency Reports.

3.7. Contractor will ensure that non-security module updates will be tested prior to implementation on a per-website basis to assure they do not break current functionality.

3.8. Contractor will not overwrite agency test site content without prior written notification and consent from agency.

3.9. Contractor will maintain a current and updated log of all test and production URLs, including current Drupal Core version, for each agency URL maintained by Contractor.

3.10. Contractor will use an OCIO approved code repository process.

3.11. Contractor will implement and maintain monitoring on all contractor-maintained websites, including monitoring for downtime and server storage utilization. Contractor will use monitors to ensure appropriate uptimes for all customers.

4. **System Administration (Back end)**

Contractor will provide System Administration for all components supporting Drupal above the operating system, including the HTTP server, PHP, database server, and Drupal Core. System Administration actions include but is not limited to the following**:**

4.1. Contractor will install and maintain all State of Iowa Drupal websites on OCIO-owned hosting instances.

4.2. Contractor will isolate each Drupal instance from all other Drupal instances and will not deploy a multi-site Drupal configuration in support of State of Iowa websites.

4.3. Contractor will provide remote administration for components above the operating system including HTTP server, PHP, database server, and Drupal core. Contractor will provide system administration services remotely, via an OCIO approved mechanism for connecting to server resources.

4.4. Contractor will not perform administration of the operating system or components below the operating system.

4.5. Contractor will generally conform to OCIO practices for patching software. OCIO relies on package management utilities (yum, apt-get) and automated updating via cron of software packages included with the EC2 instance or VM build. Additional repositories from approved sources can be requested to provide alternative versions of PHP, http (e.g., Apache) and database software (MySQL or MariaDB), etc. The packages provided may be made available upon specific request to replace those versions included in the standard build.

4.6. Contractor will use sudo to execute the designated package management utilities to perform updates of the PHP, apache, mysql, MariaDB software.

4.7. Contractor will design site directory file structures with the understanding that Linux filesystem access group ownership and permission controls will be relied on to control file and directory access. OCIO will create a group for the contractor. The contractor will request user accounts for employees requiring access that OCIO will then add to the contractor group.

4.8. Contractor may be granted sudo privileges for relevant process execution upon request to OCIO.

4.9. Contractor will create a web site backup archive file for each website, including all files required for backup. Files archives will be backed up by OCIO.

4.10. Contractor will responsibly manage allocated disk space and proactively request larger volume instances when necessary. The contractor will give 48 hour notice for proactive requests.

4.11. Contractor will establish back-up retention policies in consultation with OCIO and agency customers. Contractor will collaborate with OCIO to execute and maintain the back-up retention policies.

4.12. Contractor will not set world-writeable permissions.

4.13. Contractor is responsible for file permission and ownership decisions for application specific directories and files, including the HTTP document root, Drupal files and application user directories.

4.14. Contractor will use the Change Backup process for significant changes to production. Such changes include PHP and/or Drupal version updates, major code revision, or significant new code deployment, and changes to supporting architecture.

4.15. Contractor will collaborate with OCIO hosting staff to plan and execute updates to the operating system.

5. **Training**

Contractor will create, maintain, and support training efforts to ensure content managers and creators have the knowledge to use Drupal to update their sites and content.

5.1. Contractor will create, maintain, and update a self service training portal for content managers and other end-users to consult on basic Drupal topics, basic Google Search topics, and basic Google Analytics topics to assist in managing State websites. Formats provided in the self service portal will include, but is not limited to, recordings from training sessions, additional training videos, text-based how-to guides, and other illustrative training tools geared to provide the basic command of the Drupal system, Google Search, and Google Analytics.

5.2. Contractor will host an advanced training on specific and user-requested Drupal-related topics once a quarter. Topics will include, but not limited to, training to transition to different versions of Drupal. The trainings will be available to a set number of attendees and will require a sign-up to attend. The training will be cancelled if fewer than 5 attendees have signed up by 48 hours out from the scheduled training.

6. Performance Management

6.1. Contractor will meet with OCIO vendor manager weekly to remediate issues and provide brief status updates. Contractor will meet with OCIO vendor manager and other OCIO staff as appropriate to review performance on a quarterly basis. Contractor will meet on an ad hoc basis with technical staff to resolve issues and improve technical processes.

6.2. Good Contractor will submit all logs for review to the vendor manager for review by OCIO staff on a quarterly basis. Logs will include security remediation log (referenced in 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, and 2.18), test, production, and backup logs (referenced in 3.6, 3.8, 3.9).

6.3. Contractor performance will be measured and reviewed on a quarterly basis. Measures include:

6.3.1. Customer Satisfaction: Measured quarterly and annually to quantify customer satisfaction with 80% of customers indicating that they are satisfied

6.3.2. Request Completion: Requests in State-approved ticketing system will be completed 75% of the time within 30 days or less

6.3.3. Incident Closure: In State-approved ticketing system, 80% of incidents will be resolved and closed within 48 hours

6.3.4. Change Management: Using State-approved ticketing system to track all changes, 95% of critical patches will be implemented within 5 days of availability.

7. Reporting Requirements

7.1. Contractor will maintain a current accounting of all hours consumed against the Agreement ("Quarterly Master Report"). Contractor will additionally maintain a current accounting of all hours consumed against agency specific SOWs ("Quarterly Agency Reports"). Quarterly Master Reports and Quarterly Agency Reports will be aggregated prior to the end of the contract term into an Annual Master Report and Annual Agency Reports.

7.2. Quarterly Agency Reports will include at a minimum the following data and information:

7.2.1. A management summary outlining major accomplishments, outstanding issues, concerns

7.2.2. Citizen-Facing Website Requirements Tasks delivered (per hour/per task)

7.2.3. A summation of total hours consumed per Agency per project

7.2.4. Agency created Task Orders / Project Plans opened (include time estimates and purpose)

7.2.5. Agency created Task Orders / Project Plans closed (hours estimated vs. hours spent)

7.2.6. Agency Meetings Held / Purpose of Meeting/ Next steps identified (if any)

7.3. Contractor will provide the Quarterly Master Report to OCIO. The Quarterly Master Report will include an aggregation of data from all Agency Reports, and additionally include the following data:

7.3.1. A summation of total hours consumed

7.3.2. A summation of total hours consumed per Agency

7.3.3. A management summary outlining major accomplishments, outstanding issues, concerns

7.3.4. Prior and anticipated staffing and assignment changes

7.3.5. Outreach report detailing promotional activities undertaken by Contractor to:

7.3.5.1. Increase awareness and use of the State's Drupal Content management system;

7.3.5.2. Increase utilization of IowAccess funds by participating agencies;

7.3.5.3. Suggestions for additional outreach opportunities, approaches, or strategies.

8. Project Documentation

Contractor will work with OCIO staff to document relevant OCIO and Vendor processes to ensure project success.

8.1. Contractor will assist in documenting processes to ensure high availability of selected websites.

8.2. Contractor will assist in documenting processes used to remediate and resolve tickets in State-approved ticketing system.

8.3. Contractor will assist in documenting other processes as identified to ensure program success.

9. Development Standards

9.1. Contractor will follow Drupal development standards: https://www.drupal.org/docs/develop/standards

9.2. Contractor will use SOLID principles whenever possible when developing Drupal sites and modules.

10. Customer Support

10.1. Contractor will provide 2 hours of advanced break fix for issues each month per agency. Contractor will work with agencies to prioritize issues to be fixed. Contractor will itemize the hours worked in their monthly invoices provided to agencies.

B. FY 21 Strategic Requirements

State of Iowa Citizen-Facing Website Plan

These requirements are long term goals representing desired end states for the State of Iowa portal. The Strategic Requirements identified herein will be completed by Contractor in conformance with the timeframes established, but with exact plans to be negotiated individually with Participating Agencies, where applicable, and will be billed to Agencies consistent with the Agreement, RFP1216185012, and the Agency-specific SOW. The FY2020 Strategic Requirements for the State of Iowa Citizen-Facing Website plan include the following tasks, responsibilities, and obligations:

1. Contractor will design, develop, and implement a data privacy and cookie notification function in the Iowa Web Design System.. Contractor will obtain requirements from agencies to ensure compliance with Federal and State law. Contractor will provide a routine status report to OCIO on design, development, and implementation of the data privacy and cookie notification function.

2. Contractor will implement a feedback button in the Iowa Web Design System. Contractor will provide a routine status report to OCIO on design, development, and implementation of the feedback function.

3. Contractor will implement a link to data.iowa.gov in the Iowa Web Design System. Contractor will provide a routine status report to OCIO on the implementation of the link.

4. Contractor will facilitate a webinar for agencies to teach agencies how to embed data stories into Drupal-based websites

IN WITNESS WHEREOF, the Parties have caused their respective duly authorized representatives to execute this Amendment, which is effective as of the last date of signature hereto.

STATE OF IOWA, acting by and through the **Office of the Chief Information Officer**		**Webspec Design, LLC**	
By:	Annette M. Dunn	By:	Jeremiah Terhark
Name:	Annette M. Dunn	Name:	Jeremiah Terhark
Title:	Director	Title:	Owner
Date:	5/6/2020	Date:	5/1/2020