MARYLAND
DEPARTMENT OF
BUDGET & MANAGEMENT

LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lieutenant Governor

DAVID R. BRINKLEY
Secretary

MARC L. NICOLE
Deputy Secretary

AMENDMENT #2
TO
REQUEST FOR PROPOSALS (RFP)

GOVERNMENT EFFICIENCY AND MANAGEMENT SOLUTIONS
SOLICITATION NUMBER 050B7400006

DECEMBER 30, 2016

Ladies and Gentlemen:

The following Amendment is being issued to amend language and clarify information contained in the above-named RFP. All information contained herein is binding on all Offerors who respond to this RFP. The following change is listed below; new language has been double underlined and marked in red bold (ex. **new language**) and language deleted has been marked with a double strikeout (ex. ~~**strike out**~~).

1. Revise Section 3.1.1 (**Scope of Work – Purpose**), as follows:

6) **Business and Workforce Development Agencies**: Departments of Commerce, Housing **and Community Development**, and Labor, Licensing & Regulation, and Technology Development Corporation (TEDCO)

2. Replace the existing language in Section 3.1.1 (8) (**Scope of Work – Purpose**), as follows:

~~**8) Human Capital Management** – overarching work force vulnerabilities and management issues including, but not limited to adequacy of current work force (quantity, quality), turnover, succession planning, leave policies and management, and the ability to expeditiously recruit and retain employees when needed.~~

8) Human Capital Management – overarching work force vulnerabilities and management issues including, but not limited to the adequacy of current work force (quantity, quality), turnover levels, the need for succession planning, leave and scheduling policies, policies or procedures vulnerable to fraud or abuse, impediments to the ability to expeditiously recruit and retain employees, key drivers of overtime costs and an examination of the impediments to making any recommended changes.

45 Calvert Street, Room 145 • Annapolis, MD 21401-1907
Tel: (410) 260-7374 • Fax: (410) 974-3274 • Toll Free: 1 (800) 705-3493 • TTY Users: call via Maryland Relay
http://www.dbm.maryland.gov • Andrea.Lockett@maryland.gov

3. Revise Section 3.3.3 to insert a **new** Section 3.3.3.1 (**Security Requirements – 3.3.3.1 Information Security Requirements**), as follows:

3.3.3.1 Information Security Requirements

To ensure appropriate data protection safeguards are in place, the Contractor and any relevant subcontractor(s) shall at a minimum implement and maintain the following information technology controls at all times throughout the life of the Contract. The Contractor and any relevant subcontractor(s) may augment this list with additional information technology controls.

(a) Establish separate production, test, and training environments for systems supporting the services provided under this Contract and ensure that production data is not replicated in the test and/or training environment unless it has been previously anonymized or otherwise modified to protect the confidentiality of Sensitive Data elements.

(b) Apply hardware and software hardening procedures as recommended by the manufacturer to reduce the Contractor/subcontractor's systems' surface of vulnerability. The purpose of system hardening procedures is to eliminate as many security risks as possible. These procedures may include but are not limited to removal of unnecessary software, disabling or removing of unnecessary services, the removal of unnecessary usernames or logins, and the deactivation of unneeded features in the Contractor/subcontractor's system configuration files.

(c) Establish policies and procedures to implement and maintain mechanisms for regular internal vulnerability testing of operating system, application, and network devices supporting the services provided under this Contract. Such testing is intended to identify outdated software versions; missing software patches; device or software misconfigurations; and to validate compliance with or deviations from the Contractor's and/or subcontractor's security policy. The Contractor and any relevant subcontractor(s) shall evaluate all identified vulnerabilities for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The Department shall have the right to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under this Contract.

(d) Where website hosting or Internet access is the service provided or part of the service provided, the Contractor and any relevant subcontractor(s) shall conduct regular external vulnerability testing. External vulnerability testing is an assessment designed to examine the Contractor's and subcontractor's security profile from the Internet without benefit of access to internal systems and networks behind the external security perimeter. The

Contractor and any relevant subcontractor(s) shall evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The Department shall have the right to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under this Contract.

(e) Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under this Contract; that the anti-virus and anti-malware software is automatically updated; and that the software is configured to actively scan and detect threats to the system for remediation.

(f) Enforce strong user authentication and password control measures over the Contractor/subcontractor's systems supporting the services provided under this Contract to minimize the opportunity for unauthorized system access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with the most current State of Maryland Department of Information Technology's Information Security Policy (http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx), including specific requirements for password length, complexity, history, and account lockout.

(g) Ensure State data under this service is not processed, transferred, or stored outside of the United States.

(h) Ensure that State data is not comingled with the Contractor's and subcontractor's other clients' data through the proper application of data compartmentalization security measures. This includes but is not limited to classifying data elements and controlling access to those elements based on the classification and the user's access or security level.

(i) Apply data encryption to protect State data, especially Sensitive Data, from improper disclosure or alteration. Data encryption should be applied to State data in transit over networks and, where possible, State data at rest within the system, as well as to State data when archived for backup purposes. Encryption algorithms which are utilized for this purpose must comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2.

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

(j) Enable appropriate logging parameters on systems supporting services provided under this Contract to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information

security events as recommended by the operating system and application manufacturers as well as information security standards including the current State of Maryland Department of Information Security Policy: http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx

(k) Retain the aforementioned logs and review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and perform remediation, if required. The Department shall have the right to inspect these policies and procedures and the Contractor or subcontractor's performance to confirm the effectiveness of these measures for the services being provided under this Contract.

(l) Ensure system and network environments are separated by properly configured and updated firewalls to preserve the protection and isolation of Sensitive Data from unauthorized access as well as the separation of production and non-production environments.

(m) Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems supporting the services being provided under the Contract from unsolicited and unauthenticated network traffic.

(n) Review at regular intervals the aforementioned network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure but necessary.

(o) Ensure that the Contractor's and any subcontractor's personnel shall not connect any of their own equipment to a State LAN/WAN without prior written approval by the State. The Contractor/subcontractor shall complete any necessary paperwork as directed and coordinated with the Contract Monitor to obtain approval by the State to connect Contractor/subcontractor-owned equipment to a State LAN/WAN.

4. Revise Section 3.3.3.1 (**Security Requirements – Incident Response Requirement**) to renumber the Section as 3.3.3.**2**, as follows:

3.3.3.2 Incident Response Requirement

(a) The Contractor shall notify the Contract Monitor when any Contractor and/or subcontractor system that may access, process, or store State data or work product is subject to unintended access or attack. Unintended access or attack includes compromise by computer malware, malicious search engine, credential compromise or access by an individual or

automated program due to a failure to secure a system or adhere to established security procedures.

(b) The Contractor shall notify the Contract Monitor within one (1) Business Day of the discovery of the unintended access or attack by providing notice via written or electronic correspondence to the Contract Monitor and Procurement Officer.

(c) The Contractor shall notify the Contract Monitor within two (2) hours if there is a threat to the Contractor and/or subcontractor's systems as it pertains to the use, disclosure, and security of the State's Sensitive Data.

(d) If an unauthorized use or disclosure of any Sensitive Data occurs, the Contractor shall provide written notice to the Contract Monitor within one (1) Business Day after the Contractor's discovery of such use or disclosure and, thereafter, all information the State requests concerning such unauthorized use or disclosure.

(e) The Contractor, within one (1) Business Day of discovery, shall report to the Contract Monitor any improper or non-authorized use or disclosure of Sensitive Data. The Contractor's report shall identify:
1. the nature of the unauthorized use or disclosure;
2. the Sensitive Data used or disclosed;
3. who made the unauthorized use or received the unauthorized disclosure;
4. what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and:
5. what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.
6. the Contractor shall provide such other information, including a written report, as reasonably requested by the State.

(f) The Contractor shall comply with all applicable laws that require the notification of individuals in the event of unauthorized release of PII or other event requiring notification. In the event of a breach of any of the Contractor's security obligations or other event requiring notification under applicable law, the Contractor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the State and its officials and employees from and against any claims, damages, or other harm related to such security obligation breach or other event requiring the notification.

(g) This Section 3.3.3.1 shall survive expiration or termination of the Contract.

5. Revise Section 3.6.2 **c** (**Retainage and Invoicing – General**), as follows:

(c) Contractor may submit invoices as described in Section 3.6.2**(a)** at the schedule described in Section 3.6.3~~, until such time as a Not-to-Exceed Ceiling amount, either for Phase 1 or any Phase 2 Task Order Agreement has been reached~~. **For any Phase 2 Task Order Agreement** ~~If~~ **where** a Not-to-Exceed Ceiling has been reached, the Contractor may no longer submit invoices for additional work activity. Nonetheless, a~~s per Section 1.3,~~ the Contractor must continue to diligently perform all work activities to accomplish the specified deliverables.

6. Revise Section 3.6.3 (**Retainage and Invoicing – Invoice Submission Schedule**) to replace the existing language with a new Section 3.6.3 (a and b), as follows:

~~Contractor invoices shall be prepared, signed and submitted for approval to the Contract Monitor on a monthly basis, by the 10th day of the month for all work performed under the Contract for the prior month.~~

(a) Phase 1 work shall be invoiced according to the following schedule:

Month 1 – 10% of Contractor's Fixed Price for Focus Area upon delivery and acceptance of Deliverable 1 and Deliverables 2 and 3 for the month.

Month 2 – 10% of Contractor's Fixed Price for Focus Area upon delivery and acceptance of Deliverables 2 and 3 for the month.

Month 3 – 10% of Contractor's Fixed Price for Focus Area upon delivery and acceptance of Deliverables 2 and 3 for the month.

Month 4 – 10% of Contractor's Fixed Price for Focus Area upon delivery and acceptance of Deliverables 2 and 3 for the month.

Month 5 – 20% of Contractor's Fixed Price for Focus Area upon delivery and acceptance of Deliverables 2 and 3 for the month and Deliverable 4.

Month 6 – 20% of Contractor's Fixed Price for Focus Area upon delivery and acceptance of Deliverables 2 and 3 for the month and Deliverable 5.

Upon delivery and acceptance of Final Report (Deliverable 6) – 15% of Contractor's Fixed Price for Focus Area.

Upon completion of all Briefings (Deliverable 7) – 5% of Contractor's Fixed Price for Focus Area.

Retainage may be invoiced upon acceptance of all deliverables by Contract Monitor.

(b) Phase 2 invoicing will be as specified in each Task Order Agreement.

7. Revise Section 4.2.2 (**Volume I –Proposals**), as follows:

4.2.2 An electronic version (on Compact Disk/CD, Digital Versatile Disc/DVD, or Universal Serial Bus/USB Flash/Thumb Drive) of Volume 1-Technical Proposal in Microsoft Word format must be enclosed with the original Volume I - Technical Proposal submission. An electronic version (on CD, DVD, or USB Flash Drive) of Volume II - Financial Proposal in ~~Microsoft Word or~~ Microsoft Excel format must be enclosed with the original Volume II - Financial Proposal submission. Each CD/DVD/USB Flash Drive must be labeled on the outside with the RFP title and number, name of the Offeror, and volume number. Each CD/DVD/USB Flash Drive must be packaged with the original copy of the appropriate Proposal (Technical or Financial).

8. Revise Section 4.4.3.6 **a**, **b**, and **c** (**Offeror Technical Response to RFP Requirements and Proposed Work Plan**), as follows:

a. The Offeror shall address each Scope of Work requirement in Section 3.2 consisting of a review of each Focus Area identified in Section 3.1 in its Technical Proposal and describe how its proposed services, including the services of any proposed subcontractor(s), will meet or exceed the requirement(s). If the State is seeking Offeror agreement to any requirement(s), the Offeror shall state its agreement or disagreement. Any paragraph in the Technical Proposal that responds to a Scope of Work (Section 3.2) requirement shall include an explanation of how the work will be done. **The Offeror shall clearly explain its innovative methodology for improving State government and deriving transformational service delivery and cost efficiencies for the State.** Any exception to a requirement, term, or condition may result in having the Proposal classified as not reasonably susceptible of being selected for award or the Offeror deemed not responsible.

The Offeror shall identify and confirm specific deliverables, including frequency and timing, to be provided during Phase 1, including but not limited to: a finalized detailed project work plan, status reports (not less than monthly), progress/milestone meetings, a searchable program/services database, a Preliminary Report, a Final Report, and Briefings.

b. The Offeror shall describe its organizational structure (to include providing an organizational chart), approach, strategies and plan for managing the requirements of this RFP Section 3, including project control mechanisms. ~~The Offeror shall clearly explain its innovative methodology for improving State~~

~~government and deriving transformational service delivery and cost efficiencies for the State.~~

c. The Offeror shall provide a **separate draft Detailed Project Work Plan (Project Plan) for each Focus Area** identifying the specific proposed area of focus, personnel resources (listed by **personnel** names) to be assigned, a description of the role and functions each personnel resource is to perform, milestones to be achieved, the estimated time frame of completion of each milestone, and number of Offeror **labor hours, or level of effort (identified as a percentage of full time equivalent), by each proposed personnel resource** ~~resource/labor hours, (by labor category and personnel name)~~ for each Focus Area and task. The Project Plans should be presented with as much specificity as possible, and should incorporate and address each specific contract deliverable. Each separate Project Plan shall be numbered according to the Focus Area identified in Section 3.1.

The Offeror may identify, define and include additional Detailed Project Plans for additional Focus Areas not named in Section 3.1, which the Offeror expects will produce benefits to the State. Each Project Plan for additional Focus Areas shall include the same requirements as noted above for the 8 identified Focus Areas. The Project Plan for each additional Focus Area (not named in Section 3.1) shall be consecutively numbered beginning with number 9.

9. Revise Section 4.5.1 (**Volume II – Financial Proposal**), as follows:

4.5.1 Under separate sealed cover from the Technical Proposal and clearly identified in the format identified in Section 4.2 "Proposals," the Offeror shall submit an original unbound copy, seven (7) copies, and an electronic version in ~~Microsoft Word or~~ Microsoft Excel of the Financial Proposal. The Financial Proposal shall contain all price information in the format specified in **Attachment F**. The Offeror shall complete the Financial Proposal Form only as provided in the Financial Proposal Instructions and the Financial Proposal Form itself.

10. Replace **Attachment F (Financial Proposal Form)** to modify the 4th tab entitled D-Phase 2 to provide additional rows for the inclusion of further Labor Category(s) and Fully-Loaded Fixed Hourly Rates in the attached version.

Date Issued: December 30, 2016

By: Andrea R. Lockett
<Signed>
Procurement Officer

Attachment:
1. 050B7400006-Att F_DBM Govt. Efficiency & Mgmt Solutions RFP (Amdt 2).xlsx