

Department of General Services Website Redesign and Modernization

California Department of General Services
Request for Information
RFI# 3189571

May 6, 2016



Governor Edmund G. Brown Jr.

To: Interested Respondents

Subject: Request for Information (RFI) # 3189571, Department of General Services Website Redesign and Modernization

PURPOSE

The Department of General Services, Office of Business and Acquisition Services (DGS/OBAS) and the Department of General Services, Office of Public Affairs (DGS/OPA) are providing the opportunity for interested respondents to participate in a Request for Information (RFI) to:

- Identify a Content Management System (CMS) that will meet all of the Department's functional and technical requirements.
- Suggest a design for the external organizational website (www.dgs.ca.gov) and to ensure the proposed Scope of Work (RFI Attachment A) provides the necessary detail and accuracy to guide the design, implementation, migration, and initial support. The goal of the new website is to improve our core site's visual design, structure, navigation, content, administration and workflow.

The objective of this RFI is to gather information about current market conditions and to collect information from respondents related to the availability of goods or services that can meet the needs of the State. This is a solicitation for information only; there will be no directly resulting contract. The Questionnaire is included as Attachment B.

PLAN OVERVIEW

Once the State has reviewed the RFI responses, DGS will determine the feasibility of procurement. The intent of the Department is to contract with a third party to design, implement, migrate and provide initial support for a new external website.

KEY ACTION DATES AND TIMES

Listed below are the Key Action Dates and times within which actions should be taken or completed. If DGS/OBAS find it necessary to change any of these dates, an Addendum to this RFI will be posted on the California State Contract Register (CSCR) <https://caleprocure.ca.gov>.

Request for information (RFI) released	May 9, 2016
Last day to submit questions	April 16, 2016 by 5:00p.m. PST
Release State response to questions	May 23, 2016 by 5:00p.m. PST
Request for Information (RFI) due	May 30, 2016 by 5:00p.m. PST

Please send any RFI responses and all correspondence and/or questions related to this RFI to Jason Casillas, Acquisition Analyst, at Jason.casillas@dgs.ca.gov.

DISCLAIMER

1. This RFI is issued for information and planning purposes only and does not constitute a solicitation. A response to this RFI is not an offer and cannot be accepted by the State to form a binding contract.
2. Respondents are solely responsible for all expenses associated with responding to this RFI.
3. Participants are advised that the responses to this RFI may be subject to the Public Records Act. Please do not include any proprietary information in response to this RFI.
4. Responding to this RFI creates no obligation on the part of any respondent to the Department of General Services. Conversely, issuing this RFI and considering the responses creates no obligation on the part of the Department of General Services to any respondent.
5. Submitting a response to this RFI will not enhance the review of that respondent's proposal(s) to any future solicitations. Not submitting a response to this RFI will not prohibit a response to any future solicitation, nor disadvantage the evaluation of a response to any future solicitation. By submitting a response to this RFI a respondent is implicitly agreeing with these conditions.
6. The Department of General Services asks willing Respondents to share non-binding budgetary pricing information for each proposed solution where requested. Pricing is only for planning purposes. Any pricing provided in a response to this RFI will not be considered a proposal/bid on the part of a respondent.

RFI FORMAT AND SUBMISSION

Responses to this RFI are due by the date and time stated in the Key Action Dates section. Responses should be submitted via e-mail to the State's contact identified in the Contact Information section, and should include the following information in the e-mail subject line: **RFI # 3189571, Department of General Services Website Redesign and Modernization.**

A respondent's response shall contain the following:

1. A cover letter that includes the following elements:
 - a. Respondent name, address, telephone number, and fax number; and
 - b. Contact information including the name, title, address, phone number, fax number, and e-mail address of the respondent's primary contact person for this RFI.
2. A narrative describing the following, as applicable, if not captured in the attached questionnaire (Attachment B):
 - a. The respondent's primary business focus, areas of expertise, certifications and/or credentials relevant to the content of this RFI, and experience with similar systems; and
 - b. The respondent's experience doing business with the State of California.
3. Any additional recommendations that the respondent might find relevant to the RFI.
4. The Respondent's response to all attachments. Please ensure that the format and numbering of the response correlates to that within each attachment. Responses should be concise and

straightforward. Respondents should provide narrative, diagrams, pictures, videos and any other available means to convey their comments or answer to each specification or question, and any additional recommendations that the respondent might find relevant to this RFI.

5. The State recognizes that not all respondents will be able or willing to respond to all issues addressed in the attachments. Please respond to issues which are applicable to your company's scope of work, and indicate N/A where necessary. While not required, respondents are encouraged to answer all questions.
6. Electronic format responses must be Microsoft Word or PDF. All text, tables, and drawings must use the Microsoft Office Suite (2015 or later) and be provided in readable formats.

RESPONDENT QUESTIONS

Respondents must submit questions regarding this RFI via e-mail by the specified date identified in the Key Action Dates section. Questions should be submitted via email to the contact person listed in the Contact Information section.

The following should be included in the e-mail inquiry:

- On the subject line of the e-mail, include: **RFI # 3189571, DGS Website Redesign;**
- Respondent name, contact person, telephone number, and e-mail address, as part of the sender's contact information;
- A description of the subject or issue in question, or discrepancy found in the RFI;
- RFI section, page number, and/or other information useful in identifying the specific problem or issue in question; and
- The respondent's question(s).

At its discretion, the State may contact respondents to seek clarification of any inquiry received. The State may respond to questions directly to the respondent or if deemed necessary, release an addendum or updated RFI.

A respondent who desires clarification or further information on the content of the RFI, but whose questions relate to a proprietary aspect of that respondent's submission and if disclosed to other respondents, would expose that respondent's submission, may submit such questions in the same manner as above, marked "CONFIDENTIAL," not later than the scheduled date specified herein to ensure a response. The respondent must explain why any questions are of a sensitive nature. If OBAS concurs that the disclosure of the question or answer would expose the proprietary nature of the submission, the question will be answered and both the question and answer will be kept in confidence during the RFI process. If OBAS does not concur with the explanation of the proprietary aspect of the question(s), the question(s) will not be answered in this manner and the respondent will be so notified.

CONTACT INFORMATION

The RFI responses and all correspondence and/or questions related to this RFI shall be directed to the State contact person identified below:

Name: Jason Casillas

Office: Department of General Services

Phone: (916) 375-4229
E-mail Address: Jason.Casillas@dgs.ca.gov

BACKGROUND

Overview of DGS

The Department of General Services (DGS) serves as business manager for the State of California. DGS helps to better serve the public by providing a variety of services to state agencies through procurement and acquisition solutions, real estate management and design, environmentally friendly transportation, professional printing, design and web services, administrative hearings, legal services, building standards, oversight of structural safety, fire/life safety and accessibility for the design and construction of K-12 public schools and community colleges, and funding for school construction.

DGS is a fee-for-service agency that relies completely on revenue from billing other State entities for its services. DGS consists of multiple divisions and offices with distinct business lines.

DGS interacts with thousands of different constituents on a day-to-day basis. For these constituents, the DGS website is often the first point of contact and is vital in ensuring fast, accurate delivery of government services.

However, the design of the content management system (CMS) and user control functionality of the current DGS website are outdated and require significant changes to meet modern website standards.

For more information about DGS, visit www.dgs.ca.gov.

SCOPE

DGS seeks to redesign the external organizational website with a focus on improvements to our core site's visual design, structure, navigation, content, and workflow.

DGS is requesting that you review Attachment A – Scope of Work and reply to DGS' questionnaire, Attachment B – Questionnaire.

If there is any additional information that you would like to add that was not addressed in your response to the questionnaire, please feel free to include it.

ATTACHMENTS

Attachment A – Scope of Work

This attachment contains the scope of work for the project.

Attachment B – Questionnaire

This attachment contains questions that DGS would like answered by subject matter experts.

RFI ATTACHMENT A

PROPOSED SCOPE OF WORK

Objective

The Department of General Services (DGS) serves as business manager for the State of California. DGS helps to better serve the public by providing a variety of services to state agencies through procurement and acquisition solutions, real estate management and design, environmentally friendly transportation, professional printing, design and web services, administrative hearings, legal services, building standards, oversight of structural safety, fire/life safety and accessibility for the design and construction of K-12 public schools and community colleges, and funding for school construction.

In this multifaceted capacity, DGS interacts with thousands of different constituents on a day-to-day basis. For these constituents, the DGS website is often the first point of contact and is vital in ensuring fast, accurate delivery of government services.

DGS seeks a third party contractor to:

- Identify a Content Management System (CMS) that will meet all of the department's functional and technical requirements, and
- Redesign/rebuild the CMS-supported external website in the www.dgs.ca.gov domain; the website shall be redesigned with a focus on improvements to our core site's visual design, structure, navigation, content, administration and workflow.

Requirements

The contractor shall configure, design, develop, and implement an updated dgs.ca.gov website built upon a CMS that meets the Department's development and infrastructure standards.

1. DGS Public Website: Design, Development, and Implementation

A. DGS Website Requirements

- 1) The Contractor shall design, develop, and implement the site in a manner that meets DGS objectives of a cost-effective, easy to use, interactive, and architecturally sound website that is flexible enough to support estimated traffic load as well as projected growth in site visitors and page views.
 - a. The website design elements must adhere to the DGS Graphic Standards manual: <http://documents.dgs.ca.gov/dgsnet/logos/styleguide.pdf>
 - b. The website must adhere to applicable State of California IT Policy, Standards, Instructions and Guidelines: http://cio.ca.gov/Government/IT_Policy/
 - c. The website shall be responsively designed and compatible with the current common versions of mobile and handheld devices such as, iPhones, iPads, and Android-based smart phones and tablet computers.
 - d. The website design shall be compatible with Internet Explorer 8+, Firefox 44+, Safari 9+, Google Chrome 48+, and Android Browser 4.0+.
 - e. The website should be compliant with the requirements of the Americans with Disabilities Act as well as state Digital Accessibility Laws as described in

Statewide Information Management Manual (SIMM) Section 25:

http://www.cio.ca.gov/Government/IT_Policy/pdf/SIMM_25_IT_Accessibility_Resource_Guide_06292011.pdf

- f. The website should be compliant with the requirements of Web Content Accessibility Guidelines (WCAG) 2.0
<https://www.w3.org/TR/WCAG20/>
 - g. The website shall incorporate the following features:
 - i. Robust site search function that allows public users to search for specific content within the entire page structure.
 - ii. Ability to provide different content to different visitors based on self-reported roles or persona (customers, employees, stakeholder, etc.).
 - iii. Support for video-on-demand by embedding externally hosted videos on website pages (YouTube or similar).
 - iv. Links to live video streams.
 - v. Subscriptions, social networking, RSS, and news aggregator integration.
 - vi. Interactive tools including but not limited to Webforms, interactive image galleries, Wiki sites, blogs and commenting tools.
 - h. The website shall integrate with or incorporate a translation feature that allows users to have site content displayed in Spanish or other languages as requested.
- 2) The Contractor shall provide the following website capabilities:
- a. Ensure the website only contains advertising authorized by DGS.
 - b. Provide the ability to submit the website to search engines (i.e. Google, Bing, and Yahoo).
 - c. Provide customizable error pages.
- 3) The Contractor shall provide transition services necessary to migrate content and data from the existing web environment onto the new web environment.

B. Website Design and Customization

- 1) The Contractor shall recommend a content structure for the presentation and organization of information. DGS staff will be responsible for approving the proposal.
- 2) With an eye towards making the site visually appealing and inclusive, the contractor shall submit design specifications and design mockups with graphical elements and layout text content for DGS review, revision, and approval. DGS expects this to be an iterative process.
 - a. The contractor shall have either an in-house graphic designer or design subcontractor responsible for the graphics and visuals of the new site.
 - b. Design should be flexible and be able to be updated to a new state of California template, if a new iteration is designated by the by the Governor's Office or Department of Technology.
- 3) Upon DGS approval of design specifications and design mockups, the Contractor will develop the website. Specific tasks will include, but are not limited to, developing web page templates and user interface components, and programming dynamic web content.
- 4) The Contractor's solution shall allow the design, development, and implementation of additional features to support growth in the website functionality.

C. Accessibility and Content Testing

- 1) The Contractor shall meet the following testing requirements prior to publishing any new features, services, or sites:
 - a. Draft, submit for approval, and execute test plans for:
 - i. Broken Links
 - ii. Performance (load/stress testing)
 - iii. Internet browser/operating system compatibility
 - iv. ADA and WCAG 2.0 compliance
 - v. Site Functionality
 - vi. User Acceptance Testing
 - b. Documentation including testing process and testing results shall be submitted to a contact designated by DGS.
 - c. Test results must be reviewed and signed off by DGS.

2. Content Management System: Selection, Requirements, and Standards

A. Content Management System Functional Requirements

- 1) The Contractor shall make a recommendation on CMS that forms the foundation of the www.dgs.ca.gov solution.
 - a. The Contractor shall identify the CMS software, licenses, and any additional functional components needed to satisfy all requirements.
 - b. The website content, code/scripts/style sheets, assets, and the content management solution shall have the ability to be ported to another hosting environment with similar specifications and remain functional.
 - c. The Contractor shall provide integration functionality for access to site areas, specific content, and data.
 - i. The Contractor shall utilize the Department's Active Directory (AD) for authentication and authorization for single sign-on capabilities.
 - ii. The Contractor's solution shall allow the design, development, and implementation of additional features to support growth in the website functionality.
- 2) The Contractor shall specify an externally hosted CMS solution that meets DGS technical and developmental standards. The Contractor should use the latest available production release of industry standard tools and applications and stay current with software upgrades. Department technical requirements are as follows:
 - a. A Web CMS platform that provides non-technical users the ability to create, update, review, approve, and manage website content.
 - b. Ability to authenticate and authorize internal users through Department's AD.
 - c. Relational database that is compatible with Microsoft TSQL.
 - d. Ability to interface with internal applications and databases through Application Program Interfaces (API) and/or .NET compatible web services (e.g. WCF).
 - e. Integration with website analytics tools (e.g. Google Analytics)
 - f. Selected analytics tool needs to provide statistics on unique user site sessions, page views, hit counters, cumulative year-to-date site visits and page views, bandwidth usage, etc.
 - g. Native support for ASP.NET and C# development without an intermediary interface or middleware.
- 3) The Contractor shall configure the CMS solution to the design specifications and

mockups approved by DGS.

- a. The solution shall provide the ability for DGS staff to easily update and manage content while maintaining the uniform look and feel of the site. DGS is interested in the following features:
 - i. Authentication and authorization of DGS users through the Department's AD.
 - ii. Administration of user permissions with customizable, tiered/hierarchical permission sets and approval workflow. (e.g., CMS technical administrator, Department content authors, Department content reviewers, office-level content authors, and office-level content reviewers).
 - iii. Browser-based content authoring, approval, and publishing.
 - iv. Content creation functions, such as templating, workflow, and change management.
 - v. A content repository with basic library services, such as check-in/checkout and versioning.
 - vi. Managed delivery of content including scheduled publishing of specific content and automatically archive existing content when it is replaced.
 - vii. Integrated spelling and grammar checking tools.
 - viii. Ability to cross-post content to social media platforms, including but not limited to Facebook and Twitter.
 - ix. Ability to customize Semantic URLs, both during and after content creation within sites.
 - x. Ability to integrate/interact with third party web tools such as: Mailchimp, Wordpress, Twitter Embedded Timeline, Flickr, etc.
 - xi. Content will consist of text, link, images, videos, GIS maps, and various other document and media file formats.
 - xii. The ability to create image galleries and slideshows that can be embedded on any page.
 - xiii. Ability to query and report information from external data sources via an API or Windows Communication Foundation (WCF)
 - xiv. Ability to setup custom Cascading Style Sheets (CSS)
 - xv. Metadata or tagging system with the ability to cross-post content to multiple pages, sites and subsites.

- 4) The Contractor shall specify a variety of commercial or open source web application software architecture components that will be used to implement and operate the website. Server and disk storage hardware infrastructure must have the capability of supporting the latest available production release of each commercial or open source web application software architecture component, meeting or exceeding software manufacturer's minimum recommended system requirements.

B. Content Authoring Process and Training

- 1) DGS would like authorized DGS non-technical staff to author content, manage content, and execute workflow procedures. Some key DGS staff should have a more comprehensive ability to provide quality control and the ability to update non-routine information. DGS would like the Contractor to recommend a content management process and is open to ideas on how best to accomplish this aspect of website development and ongoing content management.
 - a. The Contractor shall conduct on-site user training, utilizing a train-the-trainer methodology, for a core team of DGS users.
 - b. The Contractor shall provide a detailed and intuitive DGS user's manual with step-

by-step instruction on how to use the CMS.

- c. The Contractor shall provide a detailed and intuitive DGS administrator's manual with step-by-step instruction on how to administrate the CMS.
 - d. The Contractor shall produce or provide videos demonstrating how to use core content authoring functionality within the CMS (e.g. how to "create a new page", "add an image gallery", "embed a video on the page", etc.).
 - e. The Contractor shall train DGS developers on how to build upon and interface with the CMS development platform.
 - f. The Contractor shall provide standards and procedures for developing and deploying custom solutions to the CMS.
 - g. The Contractor shall customize the administrative interfaces of the CMS to be more intuitive, user-friendly, and promote style consistency for content authors.
- 2) The Contractor shall proactively work with DGS to provide expertise, suggestions, and procedures for proper site promotion utilizing keyword indexing, site registration with major search engines, meta tag use, and other methods for driving traffic to the site.

C. Architectural and Integration Requirements

- 1) The system shall adhere to the DGS information system general standards, as shown in Attachment A. Exceptions to the some of the standards may be granted on a case-by-case basis for implementations that are: 1) fully vendor hosted and/or supported as evident through the vendor contract language, or 2) in the process of being upgraded to meet the standards.
- 2) Solution includes Single Sign-On integration with the DGS AD.
- 3) Solution's Role based authorization shall be AD integrated and cannot utilize database accounts.
- 4) Solution executes on an Operating System that will have security patch support for at least 3 years from the date that the project was awarded.
- 5) Solution must be compatible with all critical Operating System security patches within 90 days of the release of the security patch.
- 6) Solution must communicate over TCP/IP v4 on standard and/or clearly defined network ports. Dynamic and/or ephemeral port ranges are unacceptable.
- 7) The Solution's web based user interface must be compatible with Internet Explorer 11 in either native or compatibility mode and does not require additional Add-ons or Plug-ins.
- 8) SSL with TLS 1.2 is required for data transmission.
- 9) Data Transfer between DGS Network and "offsite hosting or cloud network:"
Input / output file size must be less than 50MB.

3. Host Environment Requirements

The Contractor shall provide or identify a hosting environment option for the CMS that meets the

system requirements defined below.

A. Host / Provider Requirements

- 1) The identified CMS shall be hosted in an external, cloud-based environment.
- 2) The host shall install all platform upgrades, patches, security updates, etc.
 - a. DGS shall be notified of all changes in accordance with the agreed upon Service Level Agreement (SLA).

B. System Availability

- 1) The Provider shall ensure that the web hosting environment including the CMS, www.dgs.ca.gov website, all networking infrastructure services and protocols required for normal web environment operation, and third-party applications/web solutions shall not experience unplanned unavailability for more than a total of 30 minutes within one calendar year in order to ensure 99.99% uptime functionality.
- 2) The Provider shall maintain 99.99% uptime of the website, CMS and web hosting environment. The hosting environment shall be functionally operational while the Provider performs maintenance or patch management.
- 3) The Provider shall utilize a system architecture that includes server redundancy to maintain 24 x 7 x 365 site operation with automatic failover to a redundant system.

C. Performance Requirements:

- 1) DGS will maintain external verification of service availability from various points on the Internet and use this data to verify conformity with the following performance requirements. The Provider shall ensure that the following web environment performance goals will be based on a controlled testing environment to benchmark and test high-speed access and processing speeds on mobile and stationary devices.
 - a. Provide Internet connectivity that will sufficiently sustain graphic-intensive pages, file transfers, and streaming audio/video clips.
 - b. The production web server must push a page in two (2) seconds or less.
 - c. The production web site's static content search engine requests shall return and download search results within four (4) seconds or less of the requesting event (e.g., user clicks "Search" or "Submit" button).
 - d. The production web site's login pages shall process user authentications and download resulting confirmation or initial secure page within four (4) seconds of the requesting event (e.g., user clicks button to submit username and password).

D. Security Requirements

- 1) The Provider shall establish and maintain security controls to protect the confidentiality, the integrity and the availability of the information, equipment, and services of the DGS web environment, including any equipment providing for high availability of web, network and security services.
 - a. The Provider shall operate in accordance with State law and policies related to the protection of information assets, and the timely and efficient management of security incidents.
- 2) The application shall adhere to the DGS security standards when storing or transmitting confidential data. DGS uses the American National Standards Institute

- (ANSI) and the FIPS standards in their information management planning and operations.
- a. The minimum security requirements of the system shall use National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A, Rev 4, at the moderate level.
 - b. State requirements as outlined in the California State Administrative Manual Section 5300, available at:
http://www.cio.ca.gov/Government/IT_Policy/pdf/SAM_Chapter_5300.pdf
 - c. If remote access is used, it must also comply with State of California, Statewide Information Management Manual (SIMM) 5360-A, Telework and Remote Access Security Standard (September 2013), available at:
http://www.cio.ca.gov/Government/IT_Policy/SIMM/SIMM5360_A.PDF.
- 3) The Provider shall establish and maintain security standards, procedures and controls to protect the data, services and availability of the telecommunications network and network equipment supporting the DGS web environment.
 - 4) The Provider shall establish and maintain security standards, procedures and controls to protect the data, services and availability of the server equipment supporting the DGS web environment. Server equipment includes web servers, application servers and database servers and may include additional servers as described in the Contractor's response to this project proposal.
 - 5) The Provider shall establish and maintain security standards, procedures and controls to protect the security and privacy of data transmissions to and from the DGS website environment.
 - 6) The Provider shall establish and maintain physical security standards, procedures and controls to protect the confidentiality, integrity and availability of the facility, the hardware, the telecommunications network and the personnel supporting the DGS website environment.
 - 7) The Provider shall make security information and controls available for use by or accessible by, staff authorized by DGS.
 - a. Security information available to DGS may include real-time access or logs from network equipment, servers, databases and software, network and application vulnerability test schedules and assessments, and security audit/review results.
 - b. Controls available to DGS may include user setup/authorization/removal, equipment configuration modification, access reporting tools, password protection of files/folders, and procedures used to request/coordinate modification to the DGS website environment.
 - 8) DGS data and structure must not be visible to other Provider customers or be available to use in Provider "general" literature and benchmarking.
 - 9) Any modification of DGS data or structure must be documented and reported immediately.
 - 10) The application shall adhere to The Federal Risk and Authorization Management Program (FedRAMP) for security assessment, authorization, and continuous monitoring.

E. Capacity Requirements

- 1) Establish secure production and testing environments with sufficient capacity to meet usage demand.
 - a. The production environment shall support 160 megabits per second bandwidth demand to accommodate normal traffic load of 10 page view per second. The production environment shall provide dynamic scalability to accommodate peak traffic demand based on usage.
 - b. The Provider shall establish and maintain a secure web testing environment with sufficient bandwidth to support 25 concurrent DGS users to test new software components or changes to software components prior to release on the production environment.
 - c. The base configuration and resources allocated to the test environment shall mirror that of the production environment.
 - d. Subsequent environment refreshes to the testing and production environment will be performed at the request of DGS staff.
- 2) Disk storage for production and testing web environment servers must provide space to accommodate future interactive functionality.

F. Backup, Recovery, and Business Continuity

- 1) The Contractor and/or Provider shall establish and maintain business continuity and disaster recovery standards, processes and procedures to support the DGS web environment objective of 99.99% uptime.
 - a. Capabilities shall include, but are not limited to, information about disaster declaration and management organization, notification and communication strategies, local and remote hosting facility recovery capabilities, recovery site telecommunications, environmental, electrical and security capacities and strategies, hardware repair and replacement strategies, staffing strategies to support site recovery, and strategy for ensuring availability and recovery of DGS web environment hardware, configuration information, applications and data.
 - b. The Contractor and/or Provider shall provide a documented business continuity plan to be implemented in case of an event or series of events that impacts the delivery of the contracted services. The business continuity plan should be current and tested annually. The business continuity plan and the results of the most recent test of the business continuity plan shall be made available to DGS upon request.
- 2) The Provider shall perform backups of the DGS data and environment for restorative and recovery purposes.
 - a. The Provider shall maintain and protect system integrity to ensure that no data is lost in the event of a service failure. Ideally, DGS would like the website database backup close to real-time, but will consider other options depending on the Proposer's cost estimate.
 - b. Full backups of DGS data must be made daily and retained for a minimum of 30 days.
 - c. At least annually and prior to any configuration changes, the Provider shall test the backup system to make sure it is working properly.
 - d. Backup data shall be available at the primary site to provide for data restoration and stored off-site in a location, outside of flood zones or other

locations prone to natural hazards, to protect against loss in the event that the primary facility is unavailable. Transportation and storage of all backup media shall be performed in a secure and environmentally controlled manner.

- e. Documentation of backup media and its location shall be kept up to date and available at both the primary and off-site locations and available to authorized DGS representatives upon request.

4. Technical Support and Service Agreements

A. Technical Support Requirements

- 1) The Provider shall supply escalation procedures and points of contact available 24 x 7 to inquire and report unplanned website outages
- 2) The Provider shall guarantee a live response that is available 24 x 7 x 365 to address and respond to service requests and resolve high priority or escalated issues.
- 3) The Provider shall assign an Account Liaison who will become familiar with the day-to-day business of the DGS environment. The liaison will serve as the primary point of contact to DGS.
- 4) The Provider shall establish and maintain server maintenance and patch management process.
 - a. Utilize a baseline analyzer to demonstrate patch level compliance to industry standards.
 - b. Utilize a change management tool to manage changes and to show which changes are made.
- 5) The Provider shall give recommendations for a website content change control process that DGS staff will follow.
 - a. Provide the ability to utilize the change management function within the Content Management System to manage changes and to show which changes are made.
- 6) The Provider shall establish and maintain a change control process for any changes to custom software, source code, and database structure.
- 7) Hosting provider representative or staff shall be available during normal DGS business hours, 6:00 a.m. to 6:00 p.m. (PT) for inquiry and recurring status update meetings.

B. Issue Logs and Reporting Agreement

- 1) The Provider shall supply an email, text messaging and/or telephone notifications for significant events within 30 minutes of such an event, as defined by DGS
 - a. Significant events will be defined by DGS and may include but are not limited to any performance degradation, web site or database availability changes, changes in software or hardware configurations, capacity utilization thresholds, and security breaches.
 - b. A writing incident report detailing: the specific characteristics and causes of each occurrence; the effect the occurrence had on service; and the steps taken to remedy the situation and prevent future occurrences shall be prepared.
 - c. The Provider shall deliver this report within 24 hours of the significant event.
- 2) The Provider shall notify DGS via phone and email, within 15 minutes of any network or server outage or any type of disruption which impacts the DGS website

entire solution; or any other occurrence that results in a failure of the functionality or inaccessibility of any area of the website.

- a. A written incident report detailing: the specific characteristics and causes of each occurrence; the effect the occurrence had on service; and the steps taken to remedy the situation and prevent future occurrences shall be prepared.
- b. The Provider shall deliver this report within 24 hours of the significant event.
- c. Service outages resulting in a client-side message indicating that the service or website is unavailable is considered a service failure and will be reported as such.

- 3) The Provider shall deliver a report, in an electronic format suitable for loading into a database, on a monthly basis, due by the 10th of the following month, as described below.
 - a. All security incidents requiring activation of the Provider's security incident response procedures within the previous month.
 - b. All incidents requiring activation of the Provider's business continuity plans within the previous month.

C. Contractor Deliverables and Turnover

- 1) The Contractor shall notify the DGS Contract Manager of any proposed changes to the Contractor's solution.
- 2) After accepting the final solution, DGS staff will take over maintenance of the content and the agreement with the hosting service provider would also be transferred to DGS
- 3) DGS staff shall be provided with copies of all source code, text, images, videos, and documentation created over the life of the project.

D. Unanticipated Tasks

- 1) In the event that additional work must be performed which was unanticipated and is not specified in this Scope of Work, but which in the opinion of both parties is necessary to the successful accomplishment of the general scope of work outlined, Unanticipated Tasks provision shall be employed.
- 2) Should an unanticipated task become a deliverable, DGS Process for Gaining Acceptance of Deliverables/Tasks shall be employed.

SOW ATTACHMENT A

DGS Information System Standards

Revised: March 21, 2016

The following Department of General Services (DGS) information system standards are requirements for all custom and commercial-off-the-shelf (COTS) system implementations. Vendor-based solutions must adhere to these standards and any vendor proposal must certify that the proposed solution will meet these standards. Exceptions to the some of the standards may be granted on a case-by-case basis for implementations that are: 1) fully vendor hosted and/or supported as evident through the vendor contract language, or 2) in the process of being upgraded to meet the standards.

General Standards

1. Solution includes Single Sign On integration with DGS Active Directory.
 2. Solution executes on an Operating System that will have security patch support for at least 3 years from the date of the RFO was issued.
 3. Solution must be compatible with all critical Operating System security patches within 90 days of the release of the security patch.
 4. Solution must communicate over TCP/IP v4 on standard and/or clearly defined network ports. Dynamic and/or ephemeral port ranges are unacceptable.
 5. The Solution's web based user interface must be compatible with Internet Explorer 11 in either native or compatibility mode.
 6. Any of the Solution's locally installed desktop applications must be compatible with Windows 7.
 7. Any network servers required by the Solution that will be hosted on the DGS's network must be:
 - Completely compatible with VMWare vSphere 5.5. There can be no physical licensing or security hardware required for the Solution's operation. For example, the Solution cannot require a USB dongle for license compliance.
 - MS Windows Server 2012 compatible.
 - MS SQL Server 2012 compatible.
 - Located physically at DGS, 707 3rd street West Sacramento CA and allow for software updates at this location.
-

Network Standards

The proposed solution must be able to be deployed on a converged network and meet or exceed the following network requirements:

1. ISO 35.110, Networking.
2. IEEE 802.3, Communication Standards.
3. ANSI/TIA-568-C.0, Generic Telecommunications Cabling for Customer Premises, 2009.
4. ANSI/TIA-568-C.1, Commercial Building Telecommunications Cabling Standard, 2009.
5. ANSI/TIA-568-C.2, Balanced Twisted-Pair Telecommunication Cabling and Components Standard, published 2009.
6. ANSI/TIA-568-C.3, Optical Fiber Cabling Components Standard, published 2008, plus errata issued in October, 2008.
7. TIA-569-B (2004; Amd 1 2009) Commercial Building Standard for Telecommunications Pathways and Spaces.
8. ANSI/TIA/EIA-606-A-2002, Administration Standard for Commercial Telecommunications Infrastructure.

Security Standards

DGS uses the American National Standards Institute (ANSI) and the FIPS standards in their information management planning and operations.

1. The minimum security requirements of the system shall use National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A, Rev 4, at the moderate level.
2. State requirements as outlined in the California State Administrative Manual Section 5300, available at:
http://www.cio.ca.gov/Government/IT_Policy/pdf/SAM_Chapter_5300.pdf
3. If remote access is used, it must also comply with State of California, Statewide Information Management Manual (SIMM) 5360-A, Telework and Remote Access Security Standard (September 2013), available at:
http://www.cio.ca.gov/Government/IT_Policy/SIMM/SIMM5360_A.PDF

RFI ATTACHMENT B

QUESTIONNAIRE

1. Based on the requirements specified in the attached "Scope of Work" document, what Content Management System would you recommend?
2. At a high level, describe the process to implement the system.
3. Have you performed work, similar to what is described in the SOW, for other public sector organizations or other large/complex organizations? If so, please provide a list of the organizations.
4. Provide a rough system architecture diagram which shows the technical components and specifies where each component is hosted in the environment (e.g. Microsoft Cloud, Amazon Cloud, etc.).
5. What types of resources, qualifications, and hours of efforts (per role) would typically be assigned to this type of project?
6. How many months do you expect it will take to complete a project of this size and magnitude?
7. Are there any features or functions that were not listed in the Scope of Work that would be useful to our customers?
8. How much training is typically required for new users, such as content owners, who are not technically savvy?
9. What type of pre- and post-implementation services does your organization provide?
10. It is anticipated that any contract resulting from this RFI would be solicited using a leveraged procurement agreement. Do you currently hold a CMAS or ITMSA agreement? If not, would you qualify? If so, here is the link to apply <https://caleprocure.ca.gov/pages/index.aspx>.