INVITATION FOR BID

FILE NO.: 8810

COMMODITY: Consumer Engagement System Software

NAME OF BIDDER: Elizabeth Unger

BIDDER'S FEDERAL ID. PH: 617-349-4310

Purchasing Agent
795 Massachusetts Avenue
Cambridge, MA 02139

The undersigned submits this sealed bid to provide the commodity or services identified above, described in the specifications herein and advertised in the CAMBRIDGE CHRONICLE on Thursday, September 19, 2019 which is to be opened and publicly read at the Office of the Purchasing Agent, City Hall, 795 Mass. Ave., Room 303, Cambridge, MA at 11:00 a.m. on THURSDAY October 3, 2019. This bid may be downloaded from the City's web site, www.CambridgeMa.gov, Online Services, Purchasing Bid List, Invitation for Bid, 8810.

The undersigned certifies that this bid is made without collusion with any other person, firm or corporation making any other bid or who otherwise would make a bid. The undersigned agrees to furnish the commodity or services in strict accordance with the bid documents, which consist of this invitation to Bid and all attachments hereto. "The submitted bid must be without conditions, exceptions or modifications to the bid document".

The envelope containing the bid must be labeled: "This envelope contains a bid for “Consumer Engagement System Software” opened at 11:00 A.M. on Thursday, October 3, 2019. The bid and all documents submitted with it are public records. Parking is limited at this location. It is strongly recommended that the bids are mailed or delivered in advanced of the due date and time. Late bids will not be accepted.

This Bid process and the award of the contract are made in conformity with M.G.L. c. 30B, unless otherwise stated.

See other side of this form for General Terms and Conditions that shall become part of any Contract awarded through this invitation to Bid.

This bid includes addenda numbered: ____________________________________________

SIGNATURE OF BIDDER: _______________________________________________________

TITLE OF SIGNATORY ____________________________

ADDRESS OF BIDDER __________________________________________________________

TELEPHONE NUMBER _________________________________________________________

EMAIL ADDRESS: ____________________________________________________________

Please check one of the following and insert the requested information:

( ) Corporation, incorporated in the State of: _______________________________________

( ) Partnership: Names of partners: _____________________________________________

( ) Individual ________________________________________________________________

Email Address: ________________________________________________________________

Name of Bidder: ____________________________
## GENERAL TERMS AND CONDITIONS

<table>
<thead>
<tr>
<th><strong>LAW</strong></th>
<th><strong>All deliveries shall conform in every respect with all applicable laws of the Federal government, Commonwealth of Massachusetts and City of Cambridge.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EQUAL OPPORTUNITY:</strong></td>
<td><strong>The Vendor in the performance of the contract shall not discriminate on the grounds of race, color, religion, national origin, age or sex in employment practices or in the selection or retention of subcontractors, and in the procurement of materials or rental of equipment. The City may cancel, terminate or suspend the contract in whole or in part for any violation of this paragraph.</strong></td>
</tr>
<tr>
<td><strong>TAXES:</strong></td>
<td><strong>Purchases made by the City are exempt from the payment of Federal excise tax and the payment of Commonwealth of Massachusetts sales tax (except for gasoline) and any such taxes must not be included in the bid prices.</strong></td>
</tr>
<tr>
<td><strong>QUANTITIES:</strong></td>
<td><strong>Unless otherwise stated, the quantities set forth herein are ESTIMATES ONLY. The City reserves the right to purchase the commodity(ies) specified in any amount less than the estimated amount.</strong></td>
</tr>
<tr>
<td><strong>BID PRICES:</strong></td>
<td><strong>Bid prices shall include transportation and delivery charges fully prepaid to the City of Cambridge destination. Where the unit price and the total price are at variance, the unit price will prevail.</strong></td>
</tr>
<tr>
<td><strong>DELIVERY AND PACKAGING</strong></td>
<td><strong>Deliveries must be made in such quantities as called for in the purchase order and in the manufacturer's original packages. All deliveries must be &quot;inside&quot; delivery with no assistance from City personnel. Tailgate deliveries will not be accepted. Rejected material will be returned to the vendor at the vendor's expense.</strong></td>
</tr>
<tr>
<td><strong>MODIFICATION OF BIDS:</strong></td>
<td><strong>Prior to bid opening, a bidder may correct, modify or withdraw its bid by making the request in writing prior to the time and date for the bid opening. All corrections and modifications must be delivered to the Purchasing Department in a sealed envelope indicating that it contains a modification or correction of the original bid submitted for the particular commodity and indicating the time and date of the bid opening.</strong></td>
</tr>
<tr>
<td><strong>REJECTION OF BIDS:</strong></td>
<td><strong>The City reserves the right to reject any and all bids if it is in best interest of the City to do so.</strong></td>
</tr>
<tr>
<td><strong>AWARD OF CONTRACT:</strong></td>
<td><strong>Contract(s) will be awarded within forty-five days of the bid opening unless award date is extended by consent of all parties concerned. The continuation of any contract into the next fiscal year shall be subject to the appropriation and availability of funds.</strong></td>
</tr>
<tr>
<td><strong>INDEMNITY:</strong></td>
<td><strong>Unless otherwise provided by law, the Vendor will indemnify and hold harmless the City against any and all liability, loss, damages, costs or expenses for personal injury or damage to real or tangible personal property which the City may sustain, incur or be required to pay, arising out of or in connection with the performance of the Contract by reason of any negligent action/inaction or willful misconduct by the Contractor, its agents, servants or employees.</strong></td>
</tr>
<tr>
<td><strong>TERMINATION OF CONTRACT:</strong></td>
<td><strong>Except as otherwise provided in the Articles of Agreement, the City may terminate the contract upon seven days notice.</strong></td>
</tr>
<tr>
<td><strong>ASSIGNABILITY:</strong></td>
<td><strong>The Vendor shall not assign, sell, subcontract or otherwise transfer any interest in this contract without the prior written consent of the City.</strong></td>
</tr>
</tbody>
</table>
| **MATERIAL SAFETY DATA SHEETS:** | **Pursuant to M.G.L. c. 111F. ss. 8, 9, and 10, any vendor who receives a contract resulting from this invitation agrees to submit a Material Safety Data Sheet for each toxic or hazardous substance or mixture containing such substance when deliveries are made. The vendor agrees to comply with all requirements set forth in the pertinent laws above.**

**Name of Bidder:** ____________________________
Elizabeth Unger, Purchasing Agent
City Hall, Cambridge, Massachusetts 02139

The undersigned hereby proposes to furnish **Consumer Engagement System Software** for the Water Department for a period of three years, all in accordance with the attached specifications and following proposal schedule.

One contract will be awarded as a result of this bid. A Contract will be awarded to the responsive, responsible bidder offering the lowest total price for Consumer Engagement System Software for a period of three years (2019 - 2021).

Contract will be awarded within sixty days of the bid opening unless award date is extended by consent of all parties concerned.

This contract will be cancelled if funds are not appropriated or otherwise not made available to support the continuation of the agreement after the **first fiscal year**.

Prior to bid opening, a bidder may correct, modify or withdraw its bid by making the request in writing prior to the time and date for the bid opening. All corrections and modifications must be delivered to the Purchasing Department in a sealed envelope with a notation on the envelope indicating that it contains a modification or correction of the original bid submitted for the particular commodity and indicating the date and time of the bid opening.

**Living Wage Requirements**
The City of Cambridge has a Living Wage Requirement that establishes minimum hourly rates for all personnel who work inside the City limits. The City of Cambridge’s Living Wage as of March 1, 2019 is $16.15 per hour. The Living Wage Requirements are attached.

**Wage Theft Certification**
In Executive Order 2016-1, the City of Cambridge established requirements for City Contract in an effort to prevent wage theft. Prospective vendors must provide certifications or disclosures with their bids/proposals. Failure to provide the certification or disclosure shall result in rejection of the bid/proposal. Please see the Wage Theft Prevention Certification form attached.

**Confidentiality and Public Records Law**
All bids or other materials submitted by the vendor in response to this Invitation to Bid will be open for inspection by any person and in accordance with the Massachusetts Public Records Law.

**Questions**
Questions concerning this Invitation to Bid must be submitted in writing and either emailed to purchasing@cambridgema.gov or delivered to the Office of the Purchasing Agent, Elizabeth Unger, City Hall, 795 Massachusetts Avenue Room 303, Cambridge, MA 02139. The deadline for questions no later than Thursday September 26, 2019 by 3:00 PM. An addendum will be issued posted to the Purchasing website notifying all bidders of the questions and answers.

Please check the website for Addendums before submitting your bid to the City. Bidders will not be notified individually of Addendums.

**Confidentiality and Public Record Law**
All bids or other materials submitted by the vendor in response to this invitation to Bid will be open for inspection by any person in accordance with the Massachusetts Public Record Law.

**Bid Results**
The tab sheet and the contract award information will not be mailed to the bidders individually. A tab sheet with the bid results will be posted to the website soon after the bid opening. The tab sheet will include the “contract award” information as soon as it is determined.
Introduction

A. Purpose

The Cambridge Water Department (CWD) is requesting bids for a web-based consumer engagement system to allow customers to view their daily water meter readings on-line.

B. Project Background

The Cambridge Water Department (CWD) uses the Aclara fixed based radio Automated Meter Reading system (AMR) and STAR software for approximately 15,750 water accounts.

C. Scope of Services

The software system shall provide the following capabilities for the City’s Consumer Engagement System Software:

- A secure cloud-based environment in which the data collected is hosted
- Ability to receive and consolidate meter readings from the Aclara AMR system and STAR software.
- A secure Consumer Engagement system that can:
  - Provide historical meter data reads
  - Provide consumption reads
  - Provide standard reports on consumption and alerts
  - Provide potential customer account leak detection capabilities
  - Ability to view water consumption monthly, weekly, daily and hourly as available from meter reading system graphically
  - Ability for customers to sign up for alerts regarding potential leaks
  - Ability for customers to sign up for alerts regarding consumption
  - Ability for customers to authenticate to the application securely using industry standard OWASP (Open Web Application Security Project) authentication guidelines listed here: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html (Appendix 1)

CWD will work with Aclara to provide access to Network Control Computer (NCC). The successful bidder will be given access to the NCC via agreed upon remote access methods. CWD will provide existing customer information (“Customer Data”) as necessary in an ASCII file format.

The successful bidder will be responsible to install and configure the Consumer Engagement software for use by CWD. In addition, they will be responsible for developing and unit testing all interfaces required for the NCC.

The successful bidder will be responsible to ensure that the Consumer Engagement software is compatible with STAR should there be any upgrades to STAR during the three-year contract duration.

The successful bidder must provide a schedule which will be reviewed and agreed upon by CWD staff during the project kick off meeting. Actual project start dates should be included in this schedule.
QUALITY REQUIREMENTS:

A “NO” response, a failure to respond, or a failure to meet any of the following Quality Requirements will result in a rejection of your bid.

Circle “YES” or “NO” for each of the following requirements:

1. Bidder has a software system which is specifically designed for Consumer Engagement System.
   
   Yes  No

2. Bidder has a minimum of three years’ experience in design of software.
   
   Yes  No

3. Bidder can provide account log-in security as described in the scope of services.
   
   Yes  No

4. Bidder will provide training and ongoing support of system for a minimum of three years.
   
   Yes  No

5. Bidder has successfully implemented a Consumer Engagement system integrated with Aclara’s STAR Software.
   
   Yes  No

6. Bidder is the developer and will remain the maintainer of this software for the duration of this contract.
   
   Yes  No

7. Bidder has staff available to begin implementation within 60 days of the fully executed contract.
   
   Yes  No

BID SUBMISSION REQUIREMENTS:

Please provide the names, telephone numbers, street addresses and email addresses of at least three references where a Consumer Engagement system including integration of Aclara’s STAR software was successfully implemented. A bid may be rejected on the basis of one or more references reporting poor past performance by the bidder. The City reserves the right to use itself as a reference.

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Contact Name</th>
<th>Job Title</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>Contact Name</td>
<td>Job Title</td>
<td>Address</td>
<td>Phone</td>
</tr>
<tr>
<td>Company Name</td>
<td>Contact Name</td>
<td>Job Title</td>
<td>Address</td>
<td>Phone</td>
</tr>
</tbody>
</table>

Name of Bidder: ____________________________
**Price Proposal**

The total bid price must be complete and include all cost associated with software licenses, implementation, training, travel, customization, and annual maintenance. Bids should cover all vendor costs for three years.

<table>
<thead>
<tr>
<th>Year</th>
<th>Per Unit Cost (if applicable)</th>
<th>Units</th>
<th>Total Annual Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Year 1</strong></td>
<td>Implementation Costs</td>
<td>1</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td>Annual License &amp; Maintenance Fee</td>
<td>15,750 customers</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td>3-day training &amp; materials</td>
<td>Up to 10 people</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL Year 1:</strong></td>
<td></td>
<td>$</td>
</tr>
<tr>
<td><strong>Year 2</strong></td>
<td>Annual License &amp; Maintenance Fee</td>
<td>1</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL Year 2:</strong></td>
<td></td>
<td>$</td>
</tr>
<tr>
<td><strong>Year 3</strong></td>
<td>Annual License &amp; Maintenance Fee</td>
<td>1</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL Year 3:</strong></td>
<td></td>
<td>$</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL COSTS FOR YEAR 1, 2 and 3:</strong></td>
<td></td>
<td>$: ____________</td>
</tr>
</tbody>
</table>

Total Bid Price in words: __________________________________________

Bidders Signature: __________________________________________

Name of Bidder: __________________________________________
Appendix 1

This appendix references OWASP authentication guidelines:
https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

Introduction

Authentication is the process of verification that an individual, entity or website is who it claims to be. Authentication in the context of web applications is commonly performed by submitting a user name or ID and one or more items of private information that only a given user should know.

Session Management is a process by which a server maintains the state of an entity interacting with it. This is required for a server to remember how to react to subsequent requests throughout a transaction. Sessions are maintained on the server by a session identifier which can be passed back and forward between the client and server when transmitting and receiving requests. Sessions should be unique per user and computationally very difficult to predict.

Authentication General Guidelines

User IDs

Make sure your usernames/userids are case insensitive. User 'smith' and user 'Smith' should be the same user. User names should also be unique. For high security applications usernames could be assigned and secret instead of user-defined public data.

Email address as a User ID

For information on validating email addresses, please visit the input validation cheat sheet email discussion.

Authentication Solution and Sensitive Accounts

- Do NOT allow login with sensitive accounts (i.e. accounts that can be used internally within the solution such as to a back-end / middle-ware / DB) to any front-end user interface
- Do NOT use the same authentication solution (e.g. IDP / AD) used internally for unsecured access (e.g. public access / DMZ)

Implement Proper Password Strength Controls

A key concern when using passwords for authentication is password strength. A "strong" password policy makes it difficult or even improbable for one to guess the password through either manual or automated means. The following characteristics define a strong password:

- Password Length
  - Minimum length of the passwords should be enforced by the application. Passwords shorter than 8 characters are considered to be weak (NIST SP800-63B).
  - Maximum password length should not be set too low, as it will prevent users from creating passphrases. Typical maximum length is 128 characters. It is important to set a maximum password length to prevent long password Denial of Service attacks.

When selecting maximum password length, limitation of hashing algorithm that will be used for hashing passwords, should be taken into consideration because some of them have a maximum password length.
• Do not truncate passwords. Make sure that every character the user types in is actually included in the password.

• Allow usage of all characters including unicode and whitespaces. There should be no password composition rules limiting the type of characters permitted.

• Ensure credential rotation when a password leak, or at the time of compromise identification.

• Include password strength meter to help users create a more complex password and block common and previously breached passwords
  o zxcvbn library can be used for this purpose. (Note that this library is no longer maintained)
  o Pwned Passwords is a service where passwords can be checked against previously breached passwords. You can host it yourself or use API.

For more detailed information check:

  • ASVS v4.0 Password Security Requirements
  • Passwords Evolved: Authentication Guidance for the Modern Era

Implement Secure Password Recovery Mechanism

It is common for an application to have a mechanism that provides a means for a user to gain access to their account in the event they forget their password. Please see Forgot Password Cheat Sheet for details on this feature.

Store Passwords in a Secure Fashion

It is critical for an application to store a password using the right cryptographic technique. Please see Password Storage Cheat Sheet for details on this feature.

Transmit Passwords Only Over TLS or Other Strong Transport

See: Transport Layer Protection Cheat Sheet

The login page and all subsequent authenticated pages must be exclusively accessed over TLS or other strong transport. The initial login page, referred to as the "login landing page", must be served over TLS or other strong transport. Failure to utilize TLS or other strong transport for the login landing page allows an attacker to modify the login form action, causing the user's credentials to be posted to an arbitrary location. Failure to utilize TLS or other strong transport for authenticated pages after login enables an attacker to view the unencrypted session ID and compromise the user's authenticated session.

Require Re-authentication for Sensitive Features

In order to mitigate CSRF and session hijacking, it's important to require the current credentials for an account before updating sensitive account information such as the user's password, user's email, or before sensitive transactions, such as shipping a purchase to a new address. Without this countermeasure, an attacker may be able to execute sensitive transactions through a CSRF or XSS attack without needing to know the user's current credentials. Additionally, an attacker may get temporary physical access to a user's browser or steal their session ID to take over the user's session.

Consider Strong Transaction Authentication

Some applications should use a second factor to check whether a user may perform sensitive operations. For more information see the Transaction Authorization Cheat Sheet.

TLS Client Authentication
TLS Client Authentication, also known as two-way TLS authentication, consists of both, browser and server, sending their respective TLS certificates during the TLS handshake process. Just as you can validate the authenticity of a server by using the certificate and asking a well-known Certificate Authority (CA) if the certificate is valid, the server can authenticate the user by receiving a certificate from the client and validating against a third party CA or its own CA. To do this, the server must provide the user with a certificate generated specifically for him, assigning values to the subject so that these can be used to determine what user the certificate should validate. The user installs the certificate on a browser and now uses it for the website.

It is a good idea to do this when:

- It is acceptable (or even preferred) that the user only has access to the website from only a single computer/browser.
- The user is not easily scared by the process of installing TLS certificates on his browser or there will be someone, probably from IT support, that will do this for the user.
- The website requires an extra step of security.
- It is also a good thing to use when the website is for an intranet of a company or organization.

It is generally not a good idea to use this method for widely and publicly available websites that will have an average user. For example, it wouldn't be a good idea to implement this for a website like Facebook. While this technique can prevent the user from having to type a password (thus protecting against an average keylogger from stealing it), it is still considered a good idea to consider using both a password and TLS client authentication combined.

For more information, see: Client-authenticated TLS handshake

### Authentication and Error Messages

Incorrectly implemented error messages in the case of authentication functionality can be used for the purposes of user ID and password enumeration. An application should respond (both HTTP and HTML) in a generic manner.

#### Authentication Responses

Using any of the authentication mechanisms (login, password reset or password recovery) an application must respond with a generic error message regardless of whether:

- The user ID or password was incorrect.
- The account does not exist.
- The account is locked or disabled.

The account registration feature should also be taken into consideration, and the same approach of generic error message can be applied regarding the case in which the user exists.

The objective is to prevent the creation of a discrepancy factor allowing an attacker to mount a user enumeration action against the application.

It is interesting to note that the business logic itself can bring a discrepancy factor related to the processing time taken. Indeed, depending on the implementation, the processing time can be significantly different according to the case (success vs failure) allowing an attacker to mount a time-based attack (delta of some seconds for example).

Example using pseudo-code for a login feature:

First implementation using the "quick exit" approach
IF USER_EXISTS (username) THEN
    password hash=HASH (password)
    IS_VALID=LOOKUP_CREDENTIALS_IN_STORE (username, password hash)
    IF NOT IS_VALID THEN
        RETURN Error ("Invalid Username or Password!")
    ENDIF
ELSE
    RETURN Error ("Invalid Username or Password!")
ENDIF

It can be clearly seen that if the user doesn't exist, the application will directly throw out an error. Otherwise, when the user exists and the password doesn't, it is apparent that there will be more processing before the application errors out. In return, the response time will be different for the same error, allowing the attacker to differentiate between a wrong username and a wrong password.

Second implementation without relying on the "quick exit" approach:

password hash=HASH (password)
IS_VALID=LOOKUP_CREDENTIALS_IN_STORE (username, password hash)
IF NOT IS_VALID THEN
    RETURN Error ("Invalid Username or Password!")
ENDIF

This code will go through the same process no matter what the user or the password is, allowing the application to return in approximately the same response time.

The problem with returning a generic error message for the user is a User Experience (UX) matter. A legitimate user might feel confused with the generic messages, thus making it hard for them to use the application, and might after several retries, leave the application because of its complexity. The decision to return a generic error message can be determined based on the criticality of the application and its data. For example, for critical applications, the team can decide that under the failure scenario, a user will always be redirected to the support page and a generic error message will be returned.

Regarding the user enumeration itself, protection against brute-force attack are also effective because they prevent an attacker to apply the enumeration at scale. Usage of CAPTCHA can be applied on a feature for which a generic error message cannot be returned because the user experience must be preserved.

Incorrect and correct response examples

Login

Incorrect response examples:

• "Login for User foo: invalid password"
• "Login failed, invalid user ID"
• "Login failed; account disabled"
• "Login failed; this user is not active"

Incorrect response examples:

Correct response example:

• "Login failed; Invalid userID or password"
Password recovery

Incorrect response examples:

- "We just sent you a password-reset link"
- "This email address doesn’t exist in our database"

Correct response example:

- "If that email address is in our database, we will send you an email to reset your password"

Account creation

Incorrect response examples:

- "This user ID is already in use"
- "Welcome! You have signed up successfully"

Correct response example:

- "A link to activate your account has been emailed to ⟨input email address⟩"

Error Codes and URLs

The application may return a different HTTP Error code depending on the authentication attempt response. It may respond with a 200 for a positive result and a 403 for a negative result. Even though a generic error page is shown to a user, the HTTP response code may differ which can leak information about whether the account is valid or not.

Error disclosure can also be used as a discrepancy factor, consult the error handling cheat sheet regarding the global handling of different errors in an application.

Prevent Brute-Force Attacks

If an attacker is able to guess passwords without the account becoming disabled due to failed authentication attempts, the attacker has an opportunity to continue with a brute force attack until the account is compromised. Automating brute-force/password guessing attacks on web applications is a trivial challenge. Password lockout mechanisms should be employed that lock out an account if more than a preset number of unsuccessful login attempts are made. Password lockout mechanisms have a logical weakness. An attacker that undertakes a large number of authentication attempts on known account names can produce a result that locks out entire blocks of user accounts. Given that the intent of a password lockout system is to protect from brute-force attacks, a sensible strategy is to lockout accounts for a period of time (e.g., 20 minutes). This significantly slows down attackers, while allowing the accounts to reopen automatically for legitimate users.

Also, multi-factor authentication is a very powerful deterrent when trying to prevent brute force attacks since the credentials are a moving target. When multi-factor is implemented and active, account lockout may no longer be necessary.

Logging and Monitoring

Enable logging and monitoring of authentication functions to detect attacks / failures on a real time basis

- Ensure that all failures are logged and reviewed
- Ensure that all password failures are logged and reviewed
- Ensure that all account lockouts are logged and reviewed
Use of authentication protocols that require no password

While authentication through a user/password combination and using multi-factor authentication is considered generally secure, there are use cases where it isn’t considered the best option or even safe. Examples of this are third party applications that desire connecting to the web application, either from a mobile device, another website, desktop or other situations. When this happens, it is NOT considered safe to allow the third-party application to store the user/password combo, since then it extends the attack surface into their hands, where it isn’t in your control. For this, and other use cases, there are several authentication protocols that can protect you from exposing your users’ data to attackers.

OAuth

Open Authorization (OAuth) is a protocol that allows an application to authenticate against a server as a user, without requiring passwords or any third-party server that acts as an identity provider. It uses a token generated by the server, and provides how the authorization flows most occur, so that a client, such as a mobile application, can tell the server what user is using the service.

The recommendation is to use and implement OAuth 1.0a or OAuth 2.0, since the very first version (OAuth1.0) has been found to be vulnerable to session fixation.

OAuth 2.0 relies on HTTPS for security and is currently used and implemented by API's from companies such as Facebook, Google, Twitter and Microsoft. OAuth1.0a is more difficult to use because it requires the use of cryptographic libraries for digital signatures. However, since OAuth1.0a does not rely on HTTPS for security it can be more suited for higher risk transactions.

OpenID

OpenID is an HTTP-based protocol that uses identity providers to validate that a user is who he says he is. It is a very simple protocol which allows a service provider-initiated way for single sign-on (SSO). This allows the user to re-use a single identity given to a trusted OpenID identity provider and be the same user in multiple websites, without the need to provide any website the password, except for the OpenID identity provider.

Due to its simplicity and that it provides protection of passwords, OpenID has been well adopted. Some of the well-known identity providers for OpenID are Stack Exchange, Google, Facebook and Yahoo!

For non-enterprise environments, OpenID is considered a secure and often better choice, as long as the identity provider is of trust.

SAML

Security Assertion Markup Language (SAML) is often considered to compete with OpenID. The most recommended version is 2.0, since it is very feature complete and provides a strong security. Like OpenID, SAML uses identity providers, but unlike OpenID, it is XML-based and provides more flexibility. SAML is based on browser redirects which send XML data. Furthermore, SAML isn’t only initiated by a service provider; it can also be initiated from the identity provider. This allows the user to navigate through different portals while still being authenticated without having to do anything, making the process transparent.

While OpenID has taken most of the consumer market, SAML is often the choice for enterprise applications. The reason for this is often that there are few OpenID identity providers which are considered of enterprise class (meaning that the way they validate the user identity doesn’t have high standards required for enterprise identity). It is more common to see SAML being used inside of intranet websites, sometimes even using a server from the intranet as the identity provider.

In the past few years, applications like SAP ERP and SharePoint (SharePoint by using Active Directory Federation Services 2.0) have decided to use SAML 2.0 authentication as an often-preferred method for single sign-on implementations whenever enterprise federation is required for web services and web applications.
See also: SAML Security Cheat Sheet

FIDO

The Fast Identity Online (FIDO) Alliance has created two protocols to facilitate online authentication: The Universal Authentication Framework (UAF) protocol and the Universal Second Factor (U2F) protocol. While UAF focuses on password less authentication, U2F allows the addition of a second factor to existing password-based authentication. Both protocols are based on a public key cryptography challenge-response model.

UAF takes advantage of existing security technologies present on devices for authentication including fingerprint sensors, cameras (face biometrics), microphones (voice biometrics), Trusted Execution Environments (TEEs), Secure Elements (SEs) and others. The protocol is designed to plug-in these device capabilities into a common authentication framework. UAF works with both native applications and web applications.

U2F augments password-based authentication using a hardware token (typically USB) that stores cryptographic authentication keys and uses them for signing. The user can use the same token as a second factor for multiple applications. U2F works with web applications. It provides protection against phishing by using the URL of the website to lookup the stored authentication key.

Session Management General Guidelines

Session management is directly related to authentication. The Session Management General Guidelines previously available on this OWASP Authentication Cheat Sheet have been integrated into the Session Management Cheat Sheet.

Password Managers

Password managers are programs, browser plugins or web services that automate management of large number of different credentials, including memorizing and filling-in, generating random passwords on different sites etc.

Web applications should at least not make password managers job more difficult than necessary by observing the following recommendations:

- use standard HTML forms for username and password input with appropriate type attributes,
- do not artificially limit user passwords to a length "reasonable for humans" and allow passwords lengths up to 128 characters,
- do not artificially prevent copy and paste on username and password fields,
- avoid plugin-based login pages (Flash, Silverlight etc.)

As of 2017 Credential Management Level 1 standard for web browsers is being developed that may further facilitate interaction between password managers and complex log-in schemes (e.g. single sign-on).
WAGE THEFT PREVENTION CERTIFICATION

In Executive Order 2016-1, the City of Cambridge established requirements for City contracts in an effort to prevent wage theft. Prospective vendors must provide the following certifications or disclosures with their bids/proposals. Failure to provide the following shall result in rejection of the bid/proposal.

Instructions for this form:

A prospective vendor must check box 1 or box 2, as applicable, as well as boxes 3-5, and must sign this Form, certifying compliance with the requirements set out in this Form. This Form must be included with the bid or proposal, and for multi-year contracts must be completed annually on the contract anniversary and filed with the Purchasing Agent.

The undersigned certifies under the pains and penalties of perjury that the vendor is in compliance with the provisions of Executive Order 2016-1 as currently in effect.

All vendors must certify that [check either box 1 or box 2, as applicable]:

1. □ Neither this firm nor any prospective subcontractor has been subject to a federal or state criminal or civil judgment, administrative citation, final administrative determination, order or debarment resulting from a violation of G.L. c. 149, G.L. c. 151, or 29 U.S.C. 201 et seq. within three (3) years prior to the date of this bid/proposal submission.

   OR

2. □ This firm, or a prospective subcontractor of this firm, has been subject to a federal or state criminal or civil judgment, administrative citation, final administrative determination, order or debarment resulting from a violation of G.L. c. 149, G.L. c. 151, or 29 U.S.C. 201 et seq. within three (3) years prior to the date of this bid/proposal submission and such documentation is included in the bid/proposal submission.

In addition, all vendors must certify each of the following:

3. □ Any federal or state criminal or civil judgment, administrative citation, final administrative determination, order or debarment resulting from a violation of G.L. c. 149, G.L. c. 151, or 29 U.S.C. 201 et seq. imposed on this firm or on any prospective subcontractor while any bid/proposal to the City is pending and, if awarded a contract, during the term of the contract, will be reported to the Purchasing Agent or other City department within five (5) days of receiving notice.

4. □ Vendors awarded a contract that have disclosed a federal or state criminal or civil judgment, administrative citation, final administrative determination, or order resulting from a violation of G.L. c. 149, G.L. c. 151, or 29 U.S.C. 201 et seq. within three (3) years prior to the date of this bid/proposal, while the bid/proposal was pending, or during the term of the contract shall, upon request, furnish their monthly certified payrolls for their City contract to the Purchasing Agent for all employees working on such contract and are required to obtain a wage bond or other suitable insurance in an amount equal to the aggregate of one year’s gross wages for all employees. Vendors subject to a state or federal debarment for violation of the above laws or prohibited from contracting with the Commonwealth are prohibited from contracting with the City, and upon a finding or order of debarment or prohibition, the City may terminate the contract.

Name of Bidder: ___________________________
5. Notice provided by the City, informing employees of the protections of Executive Order 2016-1 and applicable local, state, and federal law will be posted by this firm in conspicuous places.

Attested hereto under the pains and penalties of perjury:

(Typed or printed name of person signing)  __________________________

Signature

(Typed or printed name of person signing)  __________________________

(Name of Business)

Pursuant to Executive Order 2016-1, vendors who have been awarded a contract with the City of Cambridge must post the Massachusetts Wage and Hour Laws notice informing employees of the protections of G.L. c. 149, G.L. c. 151, and 21 U.S.C. 201 et seq. in conspicuous places. This notice can be found at http://www.mass.gov/ago/docs/workplace/wage/wagehourposter.pdf

This form must be submitted with your bid
Americans with Disabilities Act (42 U.S.C. 12131)
Section 504 of the Rehabilitation Act of 1973
Tax Compliance/Anti-Collusion Statement
Debarment Statement

The Americans with Disabilities Act (the "Act") applies to all employers of fifteen or more employees. All vendors that are subject to the Act must comply with its provisions. In further compliance with the Act, all Contractors who enter into contracts with the City are prohibited from discrimination against the City's employees, regardless of the size of the Contractor.

The Act protects against discrimination on the basis of "disability", which is defined as a physical or mental impairment that substantially limits at least one "major life activity"; discrimination against a person having a history or record of such impairment; and discrimination against an individual regarded - even if inaccurately - as having such an impairment. The Act also expressly prohibits discrimination that is based on an individual's relationship or association with a disabled person.

The Contractor shall not discriminate against any qualified employee or job applicant with a disability and will make the activities, programs and services covered by any contract awarded through this procurement readily accessible to and usable by individuals with disabilities. To be qualified for a job, or to avail oneself of the Contractor's services, the individual with the disability must meet the essential eligibility requirements for receipt of the Contractor's services or participation in the Contractor's programs or activities with or without: 1) reasonable modifications to the Contractor's rules, policies and practices; 2) removal of architectural, communication, or transportation barriers; or, 3) provisions of auxiliary aids and services.

By submitting its contract, the Contractor certifies to the City of Cambridge that it understands and will comply with all applicable provisions of the Act, including compliance with applicable provisions of Section 504 of the Rehabilitation Act of 1973, if the Contractor is receiving federal funds.

The undersigned certifies under penalties of perjury that this contract has been made and submitted in good faith and without collusion or fraud with any other person. As used in this certification, the "person" shall mean any natural person, business, partnership, corporation, union, committee, club, or other organization, entity, or group of individuals.

As required by M.G.L. c. 62C, §49A, the undersigned certifies under the penalties of perjury that the Contractor has complied with all laws of the commonwealth relating to taxes, reporting of employees and contractors, and withholding and remitting child support.

The undersigned certifies that it is not currently subject to any State or Federal debarment order.

Date: _____________________________

(Print Name of person signing bid)

(Signature & Title)

This form must be submitted with your bid
CORI COMPLIANCE FORM

Persons and businesses supplying goods and/or services to the City of Cambridge ("Vendors"), who are required by law to perform CORI checks, are further required by Section 2.112.060 of the Cambridge Municipal Code to employ fair policies, practices and standards relating to the screening and identification of persons with criminal backgrounds through the CORI system. Such Vendors, when entering into contracts with the City of Cambridge, must affirm that their policies, practices and standards regarding CORI information are consistent with the policies, practices and standards employed by the City of Cambridge as set forth in the City of Cambridge CORI Policy ("CORI Policy") attached hereto.

CERTIFICATION

The undersigned certifies under penalties of perjury that the Vendor employs CORI related policies, practices and standards that are consistent with the provisions of the attached CORI Policy. **All Vendors must check one of the three lines below.**

1. ______ CORI checks are not performed on any Applicants.

2. ______ CORI checks are performed on some or all Applicants. The Vendor, by affixing a signature below, affirms under penalties of perjury that its CORI policies, practices and standards are consistent with the policies, practices and standards set forth in the attached CORI Policy.

3. ______ CORI checks are performed on some or all Applicants. The Vendor’s CORI policies, practices and standards are not consistent with the attached CORI Policy. Please explain on a separate sheet of paper.

______________________________  ________________________________
(Typed or printed name of person  Signature
Signing quotation, bid or Proposal)

________________________________________
(Name of Business)

NOTE:  
The City Manager, in his sole discretion may grant a waiver to any Vendor on a contract by contract basis.

Instructions for Completing CORI Compliance Form:
A Vendor should not check Line 1 unless it performs NO CORI checks on ANY applicant. A Vendor who checks Line 2 certifies that the Vendor’s CORI policy conforms to the policies, practices and standards set forth in the City’s CORI Policy. A Vendor with a CORI policy that does NOT conform to the City’s CORI Policy must check Line 3 and explain the reasons for its nonconformance in writing. Vendors, who check Line 3, will not be permitted to enter into contracts with the City, absent a waiver by the City Manager.

This form must be submitted with your bid
ORDINANCE NUMBER 1312

Final Publication Number 3155. First Publication in the Chronicle on December 13, 2007.

City of Cambridge

In the Year Two Thousand and Eight

AN ORDINANCE

In amendment to the Ordinance entitled “Municipal Code of the City of Cambridge”

Be it ordained that Cambridge Municipal Code Chapter 2.112 is hereby amended by adding a new Section 2.112.060 entitled “CORI Screening by Vendors of the City of Cambridge” as follows:

Adding after Section 2.112.050 the following new sections:

SECTION 2.112.060

CORI SCREENING BY VENDORS OF THE CITY OF CAMBRIDGE

Sections:

- 2.112.061 Purpose
- 2.112.062 Definitions
- 2.112.063 CORI-Related Standards of the City of Cambridge
- 2.112.064 Waiver
- 2.112.065 Applicability

2.112.061 Purpose

These sections are intended to ensure that the persons and businesses supplying goods and/or services to the City of Cambridge deploy fair policies relating to the screening and identification of persons with criminal backgrounds through the CORI system.

2.112.062 Definitions

Unless specifically indicated otherwise, these definitions shall apply and control.

Awarding Authority means the City of Cambridge Purchasing Agent or designee.

Vendor means any vendor, contractor, or supplier of goods and/or services to the City of Cambridge.

2.112.063 CORI-Related Standards of the City of Cambridge

The City of Cambridge employs CORI-related policies, practices and standards that are fair to all persons involved and seeks to do business with vendors that have substantially similar policies, practices and standards. The City of Cambridge will do business only with vendors who, when required by law to perform CORI checks, employ CORI-related policies, practices, and standards that are consistent with policies, practices and standards employed by the City of Cambridge. The awarding authority shall consider any vendor’s deviation from policies, practices and standards employed by the City of Cambridge as grounds for rejection, rescission, revocation, or any other termination of the contract.

2.112.064 Waiver

The City Manager may grant a waiver to anyone who or which has submitted a request for waiver if it is objectively reasonable; and the City Manager, or a delegate, shall report promptly in writing to the City Council all action taken with respect to every request for a waiver and the reasons for the decision.
2.112.065 Applicability

If any provision of these sections imposes greater restrictions or obligations than those imposed by any other general law, special law, regulation, rule, ordinance, order, or policy then the provisions of these sections shall control.

In City Council January 28, 2008.
Passed to be ordained by a yea and nay vote:-
Yeas 9; Nays 0; Absent 0.
Attest:- D. Margaret Drury, City Clerk.

A true copy;

ATTEST:-

D. Margaret Drury
City Clerk
City of Cambridge CORI Policy

1. Where Criminal Offender Record Information (CORI) checks are part of a general background check for employment or volunteer work, the following practices and procedures will generally be followed.

2. CORI checks will only be conducted as authorized by Criminal History Systems Board (CHSB). All applicants will be notified that a CORI check will be conducted. If requested, the applicant will be provided with a copy of the CORI policy.

3. An informed review of a criminal record requires adequate training. Accordingly, all personnel authorized to review CORI in the decision-making process will be thoroughly familiar with the educational materials made available by the CHSB.

4. Prior to initiating a CORI check, the City will review the qualifications of the applicant to determine if the applicant is otherwise qualified for the relevant position. The City will not conduct a CORI check on an applicant that is not otherwise qualified for the relevant position.

5. Unless otherwise provided by law, a criminal record will not automatically disqualify an applicant. Rather, determination of suitability based on CORI checks will be made consistent with this policy and any applicable law or regulations.

6. If a criminal record is received from CHSB, the authorized individual will closely compare the record provided by CHSB with the information on the CORI request form and any other identifying information provided by the applicant, to ensure the record relates to the applicant.

7. If, in receiving a CORI report, the City receives information it is not authorized to receive (e.g. cases with dispositions such as not guilty or dismissal, in circumstances where the City is only authorized to receive convictions or case-pending information), the City will inform the applicant and provide the applicant with a copy of the report and a copy of CHSB’s Information Concerning the Process in Correcting a Criminal Record so that the applicant may pursue correction with the CHSB.

8. If the City of Cambridge is planning to make an adverse decision based on the results of the CORI check, the applicant will be notified immediately. The applicant shall be provided with a copy of the criminal record and the City’s CORI policy, advised of the part(s) of the record that make the individual unsuitable for the position and given an opportunity to dispute the accuracy and relevance of the CORI record.

9. Applicants challenging the accuracy of the criminal record shall be provided a copy of CHSB’s Information Concerning the Process in Correcting a Criminal Record. If the CORI record provided does not exactly match the identification information provided by the applicant, the City of Cambridge will make a determination based on a comparison of the CORI record and documents provided by the applicant. The City of Cambridge may contact CHSB and request a detailed search consistent with CHSB policy.

10. If the City of Cambridge reasonably believes the record belongs to the applicant and is accurate, then the determination of suitability for the position will be made. Unless otherwise provided by law, factors considered in determining suitability may include, but not be limited to the following:

   (a) Relevance of the crime to the position sought;
   (b) The nature of the work to be performed;
   (c) Time since the conviction;
   (d) Age of the candidate at the time of offense;
   (e) Seriousness and specific circumstances of the offense;
   (f) The number of offenses;
   (g) Whether the applicant has pending charges;
   (h) Any relevant evidence of rehabilitation or lack thereof;
   (i) Any other relevant information, including information submitted by the candidate or requested by the City.
11. The Personnel Department will assist affected departments, in assessing the suitability of candidates in accordance with paragraph 10 a through i above, to ensure consistency, fairness, and protection of employment opportunities and the public interest.

12. The City of Cambridge will notify the applicant of the decision and the basis of the decision in a timely manner.

13. CORI information shall not be disseminated or shared with any unauthorized employees or other, but shall be maintained in confidence consistent with the obligations of law.

Revised May 5, 2008
Chapter 2.121

LIVING WAGE ORDINANCE

Sections:

2.121.010  Title and Purpose
2.121.020  Definitions
2.121.030  Living Wage
2.121.040  Waivers and Exceptions
2.121.050  Notification Requirements
2.121.060  Duties of covered Employers
2.121.070  Community Advisory Board
2.121.080  Enforcement
2.121.090  Severability
2.121.100  Effective Date

2.121.010  Title and Purpose.

This Chapter shall be known as the “Cambridge Living Wage Ordinance”. The purpose of this ordinance is to assure that employees of the City of Cambridge and employees of City contractors, subcontractors and beneficiaries of tax abatements, loans, grants, subsidies and other assistance provided by the City earn an hourly wage that is needed to support a family of four.

2.121.020  Definitions.

For the purposes of this ordinance, the term:

(a) "Applicable Department" means the Personnel Department for employees of the City of Cambridge, the Purchasing Department, with the advice and assistance of the appropriate department which receives the services, for Covered Employers who contract or subcontract with the City of Cambridge, the School Department for employees, contractors and subcontractors of the School Department, and the City Manager’s Office for any other Person who is a Beneficiary of assistance other than a contract or subcontract.

(b) "Assistance" means:

(1) any grant, loan, tax incentive, bond financing, subsidy, or other form of assistance valued at least $10,000 that an employer receives by or through the authority or approval of the City of Cambridge, including, but not limited to, c. 121A tax abatements, industrial development bonds, Community Development Block Grant (CDBG) loans and grants, Enterprise Zone designations awarded after the effective date of this Chapter, and the lease of city owned land or buildings below market value; and

(2) any service contract, as defined herein, of at least $10,000 with the City of Cambridge that is made with an employer to provide services pursuant to G.L.c. 30B or other public procurement laws, awarded, renegotiated or renewed after the effective date of this Chapter.

(3) any service subcontract, as defined herein, of at least $10,000.

(c) "Beneficiary" means:

(1) any person who is a recipient of Assistance;

(2) any company or person that is a tenant or sub-tenant, leaseholder or sub-leaseholder of a recipient of Assistance, provided that said company or person employs at least 25 persons and occupies property or uses equipment or property that is improved or developed as a result of Assistance, after the effective date of this Chapter; and

(d) "Covered Employer" means the City of Cambridge or a Beneficiary of Assistance.
(e) "Covered Employee" means:
   (1) a person employed by the City of Cambridge except for persons in those positions listed in Section 2.121.040(j) of this ordinance; and
   (2) a person employed by a Covered Employer, or a person employed by an independent contractor doing business with a Covered Employer, who would directly expend any of his or her time on the activities funded by the contract or the activities for which the Beneficiary received the Assistance, except for persons in those positions listed in Section 2.121.040(j) of this ordinance.

(f) "Living Wage" has the meaning stated in Section 2.121.030.

(g) "Person" means one or more of the following or their agents, employees, servants, representatives, and legal representatives: individuals, corporations, partnerships, joint ventures, associations, labor organizations, educational institutions, mutual companies, joint-stock companies, trusts, unincorporated organizations, trustees, trustees in bankruptcy, receivers, fiduciaries, and all other entities recognized at law by the Commonwealth of Massachusetts.

(h) "Service Contract" means a contract let to a contractor by the City of Cambridge for the furnishing of services, to or for the City, except contracts where services are incidental to the delivery of products, equipment or commodities. A contract for the purchase or lease of goods, products, equipment, supplies or other property is not a "service contract" for the purposes of this definition.

(i) "Service Subcontract" means a subcontract primarily for the furnishing of services, to or for a recipient of Assistance, except where services are incidental to the delivery of products, equipment or commodities. A contract for the purchase or lease of goods, products, equipment, supplies or other property is not a "service subcontract" for the purposes of this definition.

2.121.030 Living Wage.

(a) Applicability. Covered Employers shall pay no less than the Living Wage to their employees.

(b) Amount of wage. The Living Wage shall be calculated on an hourly basis and shall be no less than $10.00, subject to adjustment as provided herein. The Living Wage shall be upwardly adjusted each year no later than March first in proportion to the increase at the immediately preceding December 31 over the year earlier level of the Annual Average Consumer Price Index for All Urban Consumers (CPI-U) Boston-Lawrence-Salem, MA - NH, as published by the Bureau of Labor Statistics, United States Department of Labor applied to $10.00.

(c) No reduction in collective bargaining wage rates. Nothing in this Chapter shall be read to require or authorize any beneficiary to reduce wages set by a collective bargaining agreement.

(d) Cuts in non-wage benefits prohibited. No Beneficiary will fund wage increases required by this Chapter, or otherwise respond to the provisions of this Chapter, by reducing the health, insurance, pension, vacation, or other non-wage benefits of any of its employees.

2.121.040 Waivers and Exceptions.

(a) Waivers. A Covered Employer may request that the City Manager grant a partial or whole waiver to the requirements of this Chapter.

(b) General Waivers. Waivers may be granted where application of this Chapter to a particular form of Assistance is found by the City Solicitor to violate a specific state or federal statutory, regulatory or constitutional provision or provisions, and the City Manager approves the waiver on that basis.

(c) Hardship Waivers for certain not-for-profit employers. An employer, who has a contract with the City of Cambridge which is not subject to the provisions of G.L. c. 30B, may apply to the City Manager for a specific waiver where payment of the Living Wage by a not-for-profit Covered Employer would cause a substantial hardship to the Covered Employer.

Name of Bidder: ____________________________________________
(d) Chapter 30B contract waivers. Prior to issuing an invitation for bids for a procurement contract subject to the provisions of G.L. c. 30B, any Applicable Department may apply to the City Manager for a waiver of the application of the Living Wage to the contract where payment of the Living Wage by a Covered Employer would make it inordinately expensive for the City to contract for the services or would result in a significant loss of services, because the contracted work cannot be segregated from the other work of the Covered Employer.

(e) General Waiver Request Contents. All General Waiver requests shall include the following:
   (1) The nature of the Assistance to which this Chapter applies;
   (2) The specific or official name of the Assistance and Assistance program, the statutory or regulatory authority for the granting of the Assistance, and a copy of that authority;
   (3) The conflicting statutory, regulatory, or constitutional provision or provisions that makes compliance with this Chapter unlawful, and a copy of each such provision; and
   (4) A factual explication and legal analysis of how compliance with this Chapter would violate the cited provision or provisions, and the legal consequences that would attach if the violation were to occur.

(f) Hardship Waiver Request Contents. All Hardship Waiver requests shall include the following:
   (1) The nature of the Assistance to which this Chapter applies;
   (2) A detailed explanation of why payment of the Living Wage would cause a substantial hardship to the Covered Employer; and
   (3) A statement of proposed wages below the Living Wage.

(g) Chapter 30B Contract Waiver Request Contents. A Chapter 30B contract waiver request shall include the following:
   (1) The nature of the Assistance to which this Chapter applies;
   (2) A detailed explanation of why the contracted work cannot be segregated from the other work of the bidding Covered Employers thereby making the cost of the contract with the payment of the Living Wage inordinately expensive or would result in a significant loss of services;

(h) Community Advisory Board review and recommendation regarding waiver requests. The Community Advisory Board, as described in Section 2.121.070 of this ordinance, shall consider waiver requests along with their supporting documentation and analysis, and may hold a public hearing to consider the views of the public before making a recommendation to the City Manager regarding the waiver request. For a hardship waiver, the Community Advisory Board shall offer an opportunity to be heard to employees of the Covered Employer. After reviewing the recommendation of the Community Advisory Board, the City Manager may approve and grant or deny all or part of a request. The City Manager may in his or her discretion grant a temporary hardship waiver pending the hearing before the Community Advisory Board. For Chapter 30B contract waivers, the Community Advisory Board shall make its recommendation to the City Manager no more than thirty days after it is notified of the request for a Chapter 30B contract waiver.

(i) Terms of exceptions. If an employer is subject to this Chapter as a result of its receipt of more than one kind of Assistance covered by this Chapter, and if the City Manager grants a waiver with respect to one form of Assistance, the City Manager need not find that this Chapter is inapplicable to the employer with respect to another form of Assistance received by the employer.

(j) Exceptions. The following positions will be excepted from the requirement of the payment of the Living Wage upon certification in an affidavit in a form approved by the Applicable Department and signed by a principal officer of the Covered Employer that the positions are as follows:
   (1) youth hired pursuant to a city, state, or federally funded program which employs youth as defined by city, state, or federal guidelines, during the summer, or as part of a school to work program, or in other related seasonal or part-time program;
   (2) work-study or cooperative educational programs;
   (3) trainees who are given a stipend or wage as part of a job training program that provides the trainees with additional services, which may include, but are not limited to, room and board, case management, or job readiness services.
(4) persons working in a recognized supported employment program that provides workers with additional services, which may include, but are not limited to, room and board, case management, counseling, or job coaching:
   (5) positions where housing is provided by the employer;
   (6) employees who are exempt from federal or state minimum wage requirements; and
   (7) individuals employed by the City of Cambridge where the employment of such individuals is intended primarily to provide a benefit or subsidy to such individuals, although the City is compensating them for work performed.

2.121.050 Notification Requirements.

All Applicable Departments shall provide in writing an explanation of the requirements of this ordinance in all requests for bids for service contracts and to all persons applying for Assistance as defined by this ordinance. All persons who have signed a service contract with the City of Cambridge or a contract for Assistance shall forward a copy of such requirements to any person submitting a bid for a subcontract on the Assistance contract.

2.121.060 Duties of Covered Employers.

(a) Notification Requirements. Covered employers shall provide each Covered employee with a fact sheet about this ordinance and shall post a notice about the ordinance in a conspicuous location visible to all employees. The fact sheet and poster shall be provided to the Covered Employer by the Applicable Department and shall include:
   (1) notice of the Living Wage amount;
   (2) a summary of the provisions of this ordinance;
   (3) a description of the enforcement provisions of the ordinance;
   (4) the name, address, and phone number of a person designated by the Applicable Department to whom complaints of noncompliance with this ordinance should be directed.

(b) Contract for Assistance. At the time of signing a contract for assistance with the City of Cambridge or with a Beneficiary, the contract must include the following:
   (1) the name of the program or project under which the contract or subcontract is being awarded;
   (2) a local contact name, address, and phone number for the Beneficiary;
   (3) a written commitment by the Beneficiary to pay all Covered Employees not less than the Living Wage as subject to adjustment under this ordinance and to comply with the provisions of this ordinance;
   (4) a list of Covered Employees under the contract with the employees' job titles;
   (5) a list of all subcontracts either awarded or that will be awarded to Beneficiaries with funds from the Assistance. Upon signing any subcontracts, the Covered Employer shall forward a copy of the subcontract to the Applicable Department.

(c) Maintenance of payroll records. Each Covered Employer shall maintain payrolls for all Covered Employees and basic records relating thereto and shall preserve them for a period of three years. The records shall contain the name and address of each employee, the job title and classification, the number of hours worked each day, the gross wages, deductions made, actual wages paid, and copies of social security wage and withholding reports, and evidence of payment thereof and such other data as may be required by the Applicable Department from time to time.

(d) Applicable Department duties. The Applicable Department shall cause investigations to be made as may be necessary to determine whether there has been compliance with this Ordinance. The Applicable Department shall report the findings of all such investigations to the Community Advisory Board.

(e) Covered Employer to cooperate. The Covered Employer shall submit payroll records on request to the Applicable Department. The Covered Employer shall permit City representatives to observe work being performed upon the work site, to interview employees and to examine the books and records relating to the payrolls being investigated to determine payment of wages.
(f) **City Assistance Reports.** Each Applicable Department shall file a City Assistance Report with the City Manager and the Community Advisory Board by July 31 of each year. The report shall include, for each Assistance package or contract approved during the preceding fiscal year:
   1. the name of the Applicable Department (awarding agency), the name of the specific program under which the Assistance was awarded, and the origin of funds for Assistance;
   2. a description of the purpose or project for which the Assistance was awarded;
   3. the name, address, and phone number of a local contact person for the Covered Employer;
   4. the total cost to the City of Assistance provided to each Beneficiary, including both face-value of Assistance, as well as revenue not collected as a result of the Assistance.

2.121.070 **Community Advisory Board.**

(a) **Purpose.** The purpose of the Community Advisory Board shall be to review the effectiveness of this Ordinance at creating and retaining Living Wage jobs, to make recommendations to the City Manager regarding the granting of Waivers to Covered Employers, to review the implementation and enforcement of this ordinance, and to make recommendations from time to time in connection therewith.

(b) **Composition.** The Community Advisory Board shall be composed of nine members and shall include representatives of labor unions, community organizations and the business community. All members will be appointed by the City Manager. Members of the Board shall serve a three-year term. Whenever a vacancy shall occur the City Manager shall appoint a replacement within thirty days of said vacancy.

(c) **Meetings.** The Community Advisory Board shall meet quarterly and in special session as required. All meetings of the Board shall be open to the public and will allow for public testimony on the uses of the City Assistance generally, and on specific instances of Assistance or proposed Assistance as received or sought by individual enterprises.

(d) **Conflict of Interest.** No member of the Community Advisory Board shall participate in any proceeding concerning a Beneficiary, a Covered Employer or a Covered Employee, or applicant for waiver or exemption, if the member or any member of his or her immediate family has a direct or indirect financial interest in the outcome of said proceeding.

2.121.080 **Enforcement.**

(a) **Enforcement powers.** In order to enforce this Chapter, the Applicable Department may, with the approval and assistance of the City Solicitor, issue subpoenas, compel the attendance and testimony of witnesses and production of books, papers, records, and documents relating to payroll records necessary for hearing, investigations, and proceedings. In case of failure to comply with a subpoena, the City may apply to a court of appropriate jurisdiction for an order requiring the attendance and testimony of witnesses and the productions of books, papers, records, and documents. Said court, in the case of a refusal to comply with any such subpoena, after notice to the person subpoenaed, and upon finding that the attendance or testimony of such witnesses or the production of such books, papers, records, and documents, as the case may be, is relevant or necessary for such hearings, investigation, or proceedings, may issue an order requiring the attendance or testimony of such witnesses or the production of such documents and any violation of the court's order may be punishable by the court as contempt therefor.

(b) **Complaint procedures.** An employee who believes that he or she is a Covered Employee or an applicant for a position to be filled by a Covered Employee who believes that his or her employer is not complying with requirements of this Chapter applicable to the employer may file a complaint with the Applicable Department or with the Community Advisory Board. Complaints of alleged violations may also be filed by concerned citizens or by the City Council.

Complaints of alleged violations may be made at any time, but in no event more than three years after the last date of alleged violation, and shall be investigated promptly by the Applicable Department. Statements written or oral, made by an employee, shall be treated as confidential and shall not be disclosed to the Covered Employer without the consent of the employee.
(c) Investigations and hearings. The Applicable Department shall investigate the complaint, and may, in conjunction with the City Solicitor, and in accordance with the powers herein granted, require the production by the employer of such evidence as required to determine compliance. Prior to ordering any penalty the applicable Department shall give notice to the employer and conduct a hearing. If at any time during these proceedings, the employer voluntarily makes restitution of the wages not paid to the employee making the complaint and to any similarly situated employees, by paying all back wages owed plus interest at the average prior year Massachusetts passbook savings bank rate, or otherwise remedies the violation alleged if the violation involves matters other than wages, then the Applicable Department shall thereafter dismiss the complaint against the employer.

(d) Remedies. In the event that the Applicable Department, after notice and hearing, determines that any Covered Employer has failed to pay the Living Wage rate or has otherwise violated the provisions of this Chapter, the Applicable Department may order any or all of the following penalties and relief:

1. Fines up to the amount of $300 for each Covered Employee for each day that the Covered Employer is in violation of this Ordinance, except if the violation was not knowing and willful, then the total fine shall not exceed the amount of back wages plus interest owed;
2. Suspension of ongoing contract and subcontract payments;
3. Ineligibility for future City Assistance for up to three years beginning when all penalties and restitution have been paid in full. In addition, all Covered Employers having any principal officers who were principal officers of a barred beneficiary shall be ineligible under this section; and
4. Any other action deemed appropriate and within the discretion and authority of the city.

Remedies in this section shall also apply to the party or parties aiding and abetting in any violation of this chapter.

(e) Private right of action. Any Covered Employee, or any person who was formerly employed by a Beneficiary, may bring an action to enforce the provisions of this Chapter to recover back pay and benefits, attorneys fees and costs, by filing suit against a Beneficiary in any court of competent jurisdiction.

(f) Remedies herein non-exclusive. No remedy set forth in this Chapter is intended to be exclusive or a prerequisite for asserting a claim for relief to enforce the right granted under this Chapter in a court of law. This Chapter shall not be construed to limit an employee’s right to bring a common law cause of action for wrongful termination.

(g) Retaliation and discrimination barred. A Covered Employer shall not discharge, reduce the compensation or otherwise retaliate against any employee for making a complaint to the City, otherwise asserting his or her rights under this Chapter, participating in any of its proceedings or using any civil remedies to enforce his or her rights under the Chapter. The City shall investigate allegations of retaliation or discrimination and shall, if found to be true, after notice and a hearing, order appropriate relief as set out in paragraphs (c) and (d) herein.

2.121.090 Severability.

In the event any provision of this ordinance shall be held invalid or unenforceable by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provisions hereof.

2.121.100 Effective Date.

This law shall be effective sixty (60) after final passage.

Living Wage Ordinance (2.121) provides, at 1.121.030(b) that the wage shall be upwardly adjusted each year no later than March 1st in proportion to the increase in the Annual Average Consumer Price Index for the prior calendar year for All Urban Consumers (CPI-U) in the Boston area, as published by the federal Bureau of Labor Statistics.

For calendar year 1999, the CPI-U increased by 2.5%. Therefore, the new living wage, as of March 1, 2000 is $10.25.

For calendar year 2000, the CPI-U increased by 4.3%. Therefore, the new living wage, as of March 1, 2001 is $10.68.

For calendar year 2001, the CPI-U increased by 4.3%. Therefore, the new living wage, as of March 1, 2002 is $11.11.

For calendar year 2002, the CPI-U increased by 2.6%. Therefore, the new living wage, as of March 1, 2003 is $11.37.
The City Council has voted to amend the section of the Living Wage Ordinance (1.121.030 (b) that provides the method for calculating cost of living increases each year. As a result of this change, the living wage as of March 30, 2003 is $11.44.

For calendar year 2003, the CPI-U increased by 3.76%. Therefore, the new living wage, as of March 1, 2004 is $11.87.

For calendar year 2004, the CPI-U increased by 2.7%. Therefore, the new living wage, as of March 1, 2005 is $12.19.

For calendar year 2005, the CPI-U increased by 3.3%. Therefore, the new living wage, as of March 1, 2006 is $12.59.

For calendar year 2006 the CPI-U increased by 3.1 %. Therefore, the new living wage, as of March 1, 2007 is $12.98.

For calendar year 2007 the CPI-U increased by 1.9 %. Therefore, the new living wage, as of March 1, 2008 is $13.23.

For calendar year 2008 the CPI-U increased by 1.9 %. Therefore, the new living wage, as of March 1, 2009 is $13.69.

For calendar year 2009 the CPI-U decreased by .67 %. Therefore, the new living wage, as of March 1, 2010 will remain at $13.69.

For calendar year 2010 the CPI-U increased by 1.57%. Therefore, the new living wage, as of March 1, 2011 is $13.90.

For calendar year 2011 the CPI-U increased by 2.71%. Therefore, the new living wage, as of March 1, 2012 is $14.28.

For calendar year 2012 the CPI-U increased by 1.58%. Therefore, the new living wage, as of March 1, 2013 is $14.51.

For calendar year 2013 the CPI-U increased by 1.37%. Therefore, the new living wage, as of March 1, 2014 is $14.71.

For calendar year 2014 the CPI-U increased by 1.61%. Therefore, the new living wage, as of March 1, 2015 is $14.95.

For calendar year 2015 the CPI-U increased by .06% Therefore the new living wage, as of March 1, 2016 is $15.04.

For calendar year 2018 the CPI-U increased by 3.29 % Therefore the new living wage, as of March 1, 2019 is $16.15.
City of Cambridge
Articles of Agreement

Commodity:
File Number:

This agreement is made and entered into this ____________, by and between the City Of Cambridge ("the CITY"), a municipal corporation organized and existing under the laws of the Commonwealth of Massachusetts, and ____________, existing under the laws of the State of ________________ ("the Contractor").

Address:
Telephone, Fax, E-mail:

Article I. Definition. "This Contract" as used herein shall mean these Articles of Agreement and "the Bid Documents," which include, but are not limited to, the instructions to bidders, the Contractor's bid or proposal, the specifications, the general conditions, the requirements, the applicable addenda, and all documents and forms submitted with the Contractor's bid or proposal that were accepted by the City.

Article II. Duration. The Contractor shall commence the performance of this contract for the period beginning on __________ and ending on __________.

Article III. Terms. The Contractor agrees to provide the services all in accordance with the bid documents (bid opening date) or (proposal if appropriate).

Contract Value:

Article IV. Payment. The City agrees to pay to Contractor the sum set forth in the Contractor's bid or proposal. Contractor shall invoice department to which it provided the service, not the Purchasing Department.

Article V. Termination. The following shall constitute events of default under this Contract requiring immediate termination: a) any material misrepresentation made by the Contractor, b) any failure by the Contractor to perform any of its obligations under this Contract including, but not limited to, the following: (i) failure to commence performance of this Contract at the time specified in this Contract due to a reason or circumstance within the Contractor's reasonable control, (ii) failure to perform this Contract with sufficient personnel and equipment or with sufficient material to ensure the completion of this Contract within the specified time due to a reason or circumstance within the Contractor's reasonable control, (iii) failure to perform this Contract in a manner reasonably satisfactory to the City, (iv) failure to promptly re-perform within reasonable time the services that were rejected by the City as erroneous or unsatisfactory, (v) discontinuance of the services for reasons not beyond the Contractor's reasonable control, (vi) failure to comply with a material term of this Contract, including, but not limited to, the provision of insurance and nondiscrimination, and (vii) any other act specifically and expressly stated in this Contract as constituting a basis for termination of this Contract.

Except as otherwise provided in the Articles of Agreement, the City may terminate the contract upon seven days notice.

Article VI. Damages. From any sums due to the Contractor for services, the City may keep for its own the whole or any part of the amount for expenses, losses and damages as directed by the Purchasing Agent, incurred by the City as a consequence of procuring services as a result of any failure, omission or mistake of the Contractor in providing services as provided in this Contract.

Article VII. Conflict. In the event there is a conflict between these Articles and the Bid Documents, the Bid Documents shall supersede these Articles.

Article VIII. Governing laws and ordinances. This Contract is made subject to all the laws of the Commonwealth and the Ordinances of the City and if any such clause thereof does not conform to such laws or ordinances, such clause shall be void (the remainder of the Contract shall not be affected) and the laws or ordinances shall be operative in lieu thereof.

Name of Bidder: _____________________________
Article IX. Performance Security. Upon execution of this Contract by the Contractor, the Contractor shall furnish to the City security for the faithful performance of this Contract in the amount of ___0%___ of the value of the bid in the form of a performance bond issued by a surety satisfactory to the city or in the form of a certified check.

Article X. Equal Opportunity. the Contractor in the performance of all work under this contract will not discriminate on the grounds of race, color, sex, age, religious creed, disability, national origin or ancestry, sexual orientation, marital status, family status, military status, or source of income in the employment practices or in the selection or retention of subcontractors, and in the procurement of materials and rental of equipment. The city may cancel, terminate or suspend the contract in whole or in part for any violation of this article.

Article XI. Assignability. the Contractor shall not assign, sell, subcontract or transfer any interest in this contract without prior written consent of the city.

In witness whereof the parties have hereto and to three other identical instruments set their hands the day and year first above written.

The City: ___________________________ The Contractor: ___________________________

Louis DePasquale
City Manager

Signature and Title

Elizabeth Unger
Purchasing Agent

Approved as to Form:

Nancy E. Glowa
City Solicitor