Exhibit "B"

CIVCAST Security

CIVCAST is a well-architected framework from front-end to back-end. CIVCAST is fully deployed on the Amazon Web Services (AWS) cloud platform.

AWS Shared Responsibility Model

AWS uses a shared responsibility model. This means:

1. AWS is responsible to provide a global secure infrastructure and foundation compute, storage, networking and database services, as well as higher level services.
2. CIVCAST is responsible for protecting the confidentiality, integrity, and availability of our data in the cloud, and for meeting specific business requirements for information protection.

In short, AWS manages the security of the cloud while CIVCAST manages the security in the cloud. Using servers as an example, AWS is responsible for facilities, physical security of the hardware, network infrastructure, and virtualization infrastructure. CIVCAST is responsible for operating systems, applications, data in transit, data at rest, data stores, credentials, and polices and configuration.

AWS provides a trustworthy foundation for enterprise systems and individual applications. The AWS secure global infrastructure and services are subject to regular third-party compliance audits.

Access Control (AWS IAM)

AWS Account

CIVCAST uses Amazon Identity Access Management (IAM) to centrally manage users, security credentials such as passwords, access keys, and permissions policies that control which AWS services and assets users can access. CIVCAST uses Amazon IAM to ensure employees, services, and applications making programmatic calls to AWS have appropriate levels of permission, but no more than that. CIVCAST uses the principle of least privilege, which means each user is allowed only enough access to perform his or her required job. Multi-factor authentication (MFA), which provides an extra level of security for sign-in credentials, is enabled on all accounts.

Non-AWS Accounts (LastPass)

CIVCAST uses LastPass for all other services and tools, such as project management, helpdesk, and version control services. When a service allows, MFA is enabled on all accounts.

Password Policy

1. Change all passwords (root and personal) annually, on January 1.
2. When possible, use Multi-Factor Authentication.
3. Use the LastPass password generation tool for all new passwords.
4. Use different passwords for different accounts.
5. Do not save passwords on your computer.
6. Do not share passwords with anyone.
7. Do not let the web browser “Remember Password.”

User Authentication (AWS Cognito)

CIVCAST uses AWS Cognito for CIVCAST user authentication.

Amazon Cognito User Pools is a standards-based Identity Provider and supports identity and access management standards, such as Oauth 2.0, SAML 2.0, and OpenID Connect. OAuth 2.0 is an open standard for access delegation used by companies such as Amazon, Google, Facebook, Microsoft, and Twitter. OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol.

Amazon Cognito supports multi-factor authentication and encryption of data-at-rest and in-transit. Amazon Cognito is HIPAA eligible and PCI DSS, SOC, ISO/EIC 27001, ISO/EIC 27017, ISO/EIC 27018, and ISO 9001 compliant.

File Storage Security (AWS S3)

Introduction

All CIVCAST files (plans, bid documents, required uploads for online bidding, and all other files) are stored in the cloud on S3, a service offered by Amazon Web Services. S3 is a storage service designed for high durability and availability. Files in Amazon S3 are automatically distributed across a minimum of three physical Availability Zones (AZs) that are typically miles apart within an AWS Region.

File Protection in Transit

Files transferred to and from S3 are accessed over HTTPS (i.e. encrypted with SSL). For maximum security, files are securely uploaded/downloaded to Amazon S3 via SSL encrypted endpoints.

File Protection at Rest

For electronic bidding, files in S3 are protected at rest. Files are encrypted with Amazon S3 Server-Side Encryption (SSE). Amazon S3 SSE uses one of the strongest block ciphers available –

256-bit Advanced Encryption Standard (AES-256). With Amazon S3 SSE, every protected object is encrypted with a unique encryption key. This object key itself is then encrypted with a regularly rotated master key. Amazon S3 SSE provides additional security by storing the encrypted data and encryption keys in different hosts.

Durability and Reliability

Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 helps maintain the durability of the objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

File Access

Files stored in S3 are restricted by default. CIVCAST uses AWS IAM Policies to control access to files. Only CIVCAST APIs with proper IAM permissions can access files.

Database Security (Mongo Atlas)

CIVCAST protects data both in transit and at rest.

Introduction

CIVCAST uses MongoDB, a widely-used and highly-scalable NOSQL database. CIVCAST uses MongoDB Atlas, a cloud-based database service used by numerous government, financial, and corporate clients with enterprise-level database needs. With MongoDB Atlas, our databases are deployed in a unique Virtual Private Cloud (VPC) on AWS.

Data Protection in Transit

MongoDB Atlas uses IP whitelisting.

CIVCAST uses Secure Socket Layer (SSL) for in transit encryption between the client browser and the CIVCAST application on AWS.

Data Protection at Rest

For electronic bidding, unit prices and extended prices undergo an additional layer of encryption. Values are encrypted using 256-bit Advanced Encryption Standard (AES-256). AES was developed by the National Institute of Standards and Technology (NIST). AES has been adopted by the U.S. government to protect classified information and is used worldwide.

Sealed Bids

In addition to the encryption of unit prices and extended prices (see above), bids are sealed in a “virtual lockbox” until the date and time of the bid opening. Bids cannot be opened until the bid date and time. Also, measures are in place that prevent backdating the bid date to “peek” at bids. First, when bids are opened all bidders are immediately notified. Second, bids cannot be resealed. Once bids are open, the bid becomes stale (i.e. the bid is over).