CHALLENGE.GOV: INFORMATION SECURITY

Challenge.gov is Hosted Securely and Follows Clear Development Best Practices.

Anyone who uses Challenge.gov can be confident that their information is being stored safely and securely.

The infrastructure for Challenge.gov is hosted within the Amazon EC2 Cloud, which is a cloud environment—the same one used to host Recovery.gov. Virtual servers are accessed through SSH keys and IP filtering. The Amazon hosting environment has undergone a SAS-70 Type II audit—a third-party review of existing control procedures—which indicates a high level of IT security. GSA signed a non-disclosure agreement and reviewed this report; although it is confidential, much of the relevant information is also publicly available in Amazon's EC2 Security White Paper.

GSA's modified Terms of Service with ChallengePost includes the following provision:

> **Security Controls**: ChallengePost will, in good faith, exercise due diligence using generally accepted commercial business practices for IT security, to ensure that systems are operated and maintained in a secure manner, and that management, operational and technical controls will be employed to ensure security of systems and data. A SAS 70 Type II audit certification will be conducted annually, and ChallengePost agrees to provide GSA with the SAS 70 Type II audit certification upon the agency's request. Recognizing the changing nature of the Web, ChallengePost will continuously work with users to ensure that its products and services meet users' requirements for security of systems and data.

Challenge.gov was developed using Ruby on Rails, an open source web application framework. To ensure the security of the application, GSA interviewed ChallengePost managers about their engineering practices, configuration management, system architecture, and patching and upgrades processes. GSA found that ChallengePost incorporates IT security considerations in the development and implementation of their software applications and in the design of their virtual architectures, and found reasonable effort and attention on IT security in the design and implementation of the ChallengePost applications. Given the public posture of the data and that the data is rated "low" in the categories of confidentiality, integrity and availability, these controls should provide an adequate level of comfort with the overall system.

Vulnerability scans revealed few critical and high vulnerabilities, and most of these were mitigated during GSA's review. After the final scan, only the following vulnerabilities listed below remained which will continue to be mitigated:

	Critical/High	Medium	Low	Info/Best Practice
OS (Virtual Servers)	0	0	2	2
Application	0	0	18	86
Database	0	2	0	0

These are high scores and indicate a well-secured system. GSA finds that ChallengePost addresses IT Security risks to minimize and mitigate vulnerabilities. When IT Security issues are identified, ChallengePost reacts quickly to address potential issues. Agencies should rely on their existing IT security protections when accessing Challenge.gov in order to review solution submissions.

FACTS AT A GLANCE

- The information contained by Challenge.gov has been rated as low-risk in terms of confidentiality, integrity, and availability.
- Challenge.gov is hosted securely on Amazon's EC2 Cloud—the same service that hosts Recovery.gov.
- The Amazon EC2 Cloud has passed a SAS 70 Type II review, which GSA has reviewed, which documents how the service protects and stores information.
- The government's amended Terms of Service with ChallengePost explicitly addresses IT security needs.
- A review of ChallengePost's development practices revealed a high level of attention to security in the design and implementation of Challenge.gov.
- After multiple application-level security scans, nearly all issues found during GSA's initial review of Challenge.gov have been mitigated. No critical/high issues remain outstanding.

Additional questions? E-mail us!
challenge@gsa.gov