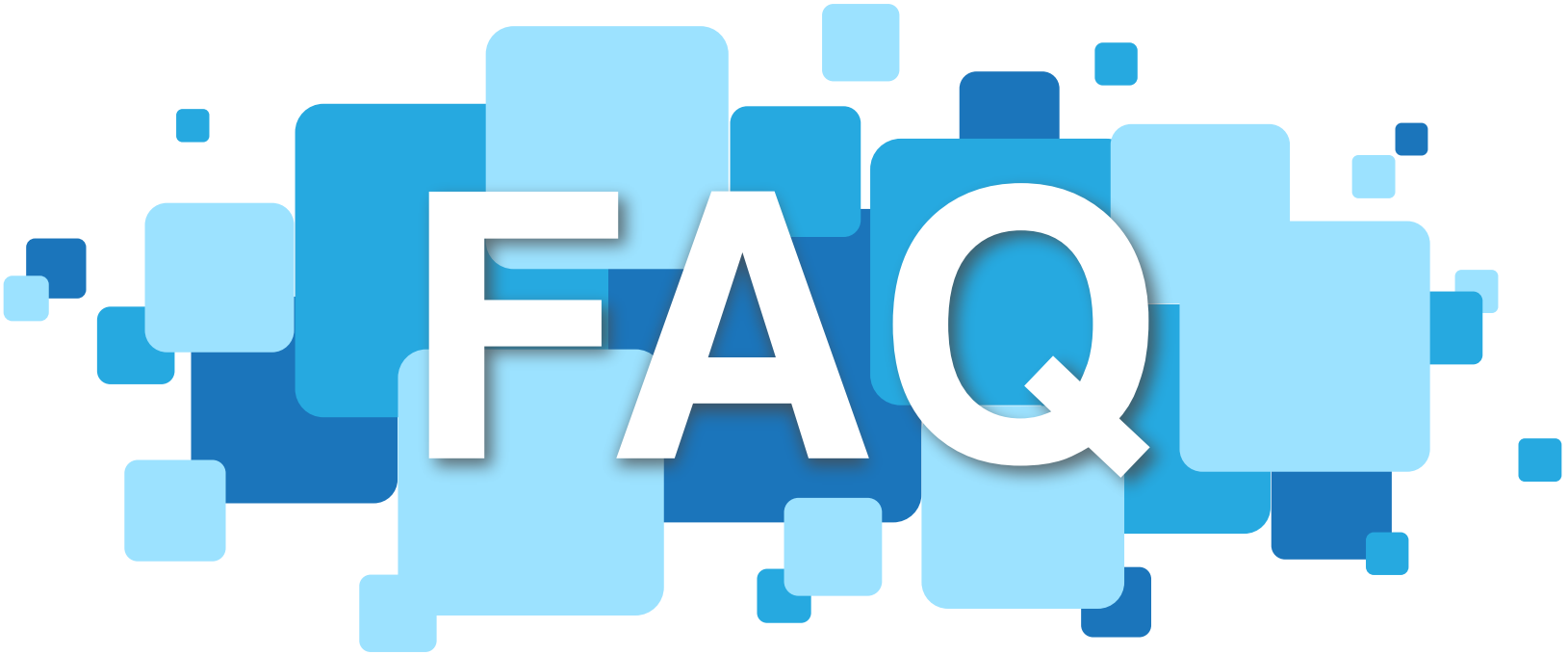
MHS
Beyond Assessments



GEARS PORTAL FAQ

MHS
Beyond Assessments

Environment Criteria

Infrastructure

- Describe the type of infrastructure being proposed (Cloud, Virtual On-Premise, Physical Hardware, or Hybrid)?
    - GEARS is hosted on AWS, which is a a cloud-based solutions. The AWS Global Infrastructure is designed and built to deliver the most flexible, reliable, scalable, and secure cloud computing environment with the highest quality global network performance. Every component of the AWS infrastructure is designed and built for redundancy and reliability, from regions to networking links to load balancers to routers and firmware. AWS infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of customers' data.

Network Transport - Connection Type

- Describe the Network Connection bandwidth for servers and workstations (e.g., 100MB, 1GB, or 10GB) required.
    - There are no specific requirements for the GEARS platform. Having low bandwidth or slow internet at the location of administration could result in slower load times if an institution has thousands of evaluations, clients, and users. This may cause minor wait times (e.g., +/- 30 seconds to load a report).

Network Transport - Application Behavior

- Describe the testing that is performed with your solution for firewalls, intrusion protection systems or other security systems.
    - GEARS is hosted on AWS, which enables the ability to build a secure, high-performing, resilient, and efficient infrastructure for the GEARS application. AWS Firewall Manager automatically enforces mandatory security policies that are defined across existing and newly created resources. The service discovers new resources as they are created across accounts. For example, if you are required to meet US Department of Treasury's Office of Foreign Assets Control (OFAC) regulations, Firewall Manager can be used to deploy an AWS WAF rule to block traffic from embargoed countries across your Application Load Balancer, API Gateway, and Amazon CloudFront accounts.

Network Transport - Access Layer Changes

- Describe any required changes in the access layer of network transport (additional vLAN's, new isolated network, redesign or rework of existing network, etc.).
    - GEARS requires an isolated private network for the application servers and a public facing network for the load balancers. The application servers are only directly accessible through a bastion host, which is only online when necessary access is required. The application servers can also receive forwarded web requests from the load balancers and only from the network the load balancers reside in.

Wireless Services

- Describe the wireless services this solution utilizes and the encryption method(s) for transmission.
    - GEARS uses the most up to date Amazon Linux distribution, currently 4.12.0

Operation System (OS)

- Describe the Operating System(s) and OS release(s) which GEARS can run.
    - We use the most up to date Amazon Linux distribution currently 4.12.0. While it is theoretically possible for the product to support running on Windows, it would require code changes in certain aspects of the system expecting a Unix based OS (Linux or MacOS).

Antivirus/Malware

- Describe the Antivirus/Malware solution(s) used.
    - ClamAV is used to scan all user submitted / uploaded files and data. The virus definition updates are checked for and applied every 3 hours.

Database (DB)

- Describe the database(s) and DB release(s) .
    - GEARS utilizes AWS' DynamoDB data base. Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multiregion, multimaster, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second. Amazon DynamoDB is a NoSQL database that supports key-value and document data models, and enables developers to build modern, serverless applications that can start small and scale globally to support petabytes of data and tens of millions of read and write requests per second. DynamoDB is designed to run high-performance, internet-scale applications that would overburden traditional relational databases.

Reporting Tools

- Describe the reporting packages that are included.
    - Amazons CloudTrail and CloudWatch to report all actions and requests that happen on every server and the Amazon Account.second. DynamoDB is designed to run high-performance, internet-scale applications that would overburden traditional relational databases.

Application Criteria

Compliance

- Describe the legal standards your solution complies with (e.g. HIPAA, PCI, CJIS, SOC 2, etc.).
    - All data from the GEARS platform are housed in an Amazon Web Services (AWS) facility within the sovereign territory of the United States of America. Data security and compliance

with state and federal data protection, domicile, and use regulations and policies are well addressed by this platform and its host environment.
With regard to specific requirements of how the data is stored and accessed in the data centre (e.g., encryption at rest and in transit, access management, password security), MHS offers a suite of solutions that ensure regional compliance requirements are met and maintained prior to, and during, the use of the GEARS platform.

Application Type

- Describe the application type (e.g. SaaS, web application, thick client, etc.).
    - GEARS is best described as Software as a Solution.

Custom Programming

- If custom programming is needed, describe the language(s) used.
    - GEARS is programmed using HTML, CSS, Javascript.

Authentication / Authorization Method(s)

- Describe the type of Authentication method that is utilized (e.g. Microsoft AD, LDAP, SAML, etc.).
    - GEARS use oAuth 2.0 protocol with Amazon Cognito to handle authentication and authorization.

Data Criteria

Data Security

- Describe what encryption is to be used, and in what form (at rest, in transit, or both).
    - All data including backups are encrypted at rest to prevent unauthorized access. When a new storage device is presented or created it has been wiped. Techniques detailed in NIST 800-88 Guidelines for Media Sanitization are used.

Backup and Recovery

- Describe the method for backup and recovery (Cloud, Disk to Disk, Disk to Tape, etc.).
    - GEARS opeates on Amazon Web service which is a cloud based solution. Backups are performed every 24 hours and retained for 7 days. All data including backups are encrypted at rest to prevent unauthorized access. When a new storage device is presented or created it has been wiped. Techniques detailed in NIST 800-88 Guidelines for Media Sanitization are used.

Retention and Purge

- Describe the standard data retention and purge proposed for your solution.
    - GDPR zip data requests are stored for seven days before they are automatically purged. If a user requests data to be expunged or purged, it is permanently removed and purged. Entire database backups are retained for 7 days, so in the event a user requests to reverse an

expungement or purge, they have 7 days to do so, however, each day that passes by Is one less backup that exists with that data. After 7 days, recovery from a user expungement/purge

Client Criteria

Network Transport – Workstation Location(s)

- Describe the Client connections (LAN, WAN, or Internet based).
    - This solution is Internet based.

Internet Browser

- Describe the browser(s) and version(s) supported.
    - GEARS may be accessed through all common web browser applications (e.g., Safari, Microsoft edge, Internet explorer, Mozilla firefox, Chrome, Safari)

Client (Workstation) Hardware / Software

- Describe the workstation requirements including Operating System, hardware requirements, and any additional software required.
    - An internet connection is all that is required to access GEARS. Personal workstation security requirements would be determined by the client.

Local Workstation Security

- Describe the workstation security requirements.
    - GEARS is password protected. This is generated by the user and is authenticated through the