GEARS PLATFORM - FAQ

Document Version Date: 12/04/2019, Jan 1/11/2020

Criteria	FAQ	
Environment		
Infrastructure	Describe the type of infrastructure being proposed (Cloud, Virtual On-Premise, Physical Hardware, or Hybrid). If the proposed solution is non-Cloud, provide the server specifications.	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 available today. 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. Security at AWS starts with our core infrastructure. Custom-built for the cloud and designed to meet the more stringent security requirements in the world, AWS infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of our customers' data. MHS offers a series of tools and services that can help any organization can build on the most secure global infrastructure, including the ability to encrypt it, move it, and manage retention.
Network Transport - Connection Type	Describe the Network Connection bandwidth for servers and workstations (e.g., 100MB, 1GB, or 10GB) required for your solution. Describe if there are any special network requirements for the solution (e.g., Latency, Jitter, etc.).	There are no specific requirements for the GEARS platform. Low bandwidth/slow internet could be noticable, but it this would simply result in slower load times for a lot of information if an institution has thousands of evaluations, clients, and users. Even still that is unlikely to cause overt or drastic delays that would impact productivity, These would be 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 MHS to build a secure, high-performing, resilient, and efficient infrastructure for the GEARS application. AWS security services and solutions are focused on delivering the following key strategic benefits critical to helping you implement your organization's optimal security posture. 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, MHS can use Firewall Manager to deploy an AWS WAF rule to block traffic from embargoed countries across your Application Load Balancer, API Gateway, and Amazon CloudFront accounts.

Criteria	FAQ	
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 our 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) on which your solution/product 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) with which your solution/product will function.	We use ClamAV 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) with which your solution/product will operate.	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 with your solution/product.	We utilize Amazons CloudTrail and CloudWatch to report all actions and requests that happen on every server and the Amazon Account.
Application		
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.

Criteria	FAQ	
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		
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.). Describe who is responsible for the backup and recovery.	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.
Recovery Time Objective (RTO) and Recovery Point Objective (RPO)	Describe your standard Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the solution.	We currently utilize Amazons Availability Zones with "hot" ready to fire database and application servers. This keeps the application resistant and automatically recoverable in the event of a server crash or failure. Database backups are done every day with a maximum of 1 day possible data loss In the event of all hot servers and other resources failing, We estimate a minimum of 24 hours required to completely recover the system and re-deploy everything with new resources from the latest backup.
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 request is impossible.
Client		

Criteria	FAQ	
Network Transport – Workstation Location(s)	Describe your Client connections (LAN, WAN, or Internet based). If peer to peer connections are required, explain why.	This solution is Internet based.
Internet Browser	Describe the browser(s) and version(s) you support.	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. Persponal workstation security requirements would be determined by torganizational policy.
Local Workstation Security	Describe the workstation security requirements for your solution.	GEARS is password protected. This is generated by the user and is authenticated through the user's email.
Maintenance		
Application Updates	Describe your release and patch cycles.	The GEARS platform is a cloud-based solution that operates independently of existing system and may be accessed through any web browser. Any upgrades to the system are completed during scheduled down time of the site. Users re provided ample notification (most commonly a week in advance) of any scheduled down time. Maintenance is generally performed during low traffic times such as evenings and weekend.
Monitoring and Alerting	Describe monitoring and alerting options provided by your solution.	The GEARS platform is a cloud-based solution that operates independently of existing system and may be accessed through any web browser. Any upgrades and patches to the system are completed during scheduled down time of the site. Users are provided ample notification (most commonly a week in advance) of any scheduled down time. Maintenance is generally performed during low traffic times such as evenings and weekend.