**Overview**

This document presents several possible scenarios for migrating highway plan scanning operation from the WV GIS Technical Center to in-house operations at DOT. Four scenarios are presented, however, they are not all-encompassing and other alternatives may be possible.

For this discussion there are 4 types of software services to consider: Database, ArcGIS, Web site hosting, and File storage.

1. **Database services** include the hosting of two databases; one that records scanning activity and as second ESRI enterprise geodata database used to support mapping activities. Both the scanning database and the geodatabase are currently implemented using Microsoft SQL Server. Operations staff must have access to the databases. Currently, operators connect directly to the geodata database using ArcMap/ArcPro and to the scanning database using a Microsoft Access front end.
2. **ArcGIS service** is an ArcGIS Server process serving of ESRI Feature and Map services. This service requires a connection to the geodatabase service.
3. **Web site hosting service** is the software used to host the DOT Highway Plans Locator website (<https://mapwv.gov/dotplans/index.php>) and the DOT Highway Plans Viewer website (<https://www.mapwv.gov/dotplans/viewer>). Currently, the websites are hosted using Microsoft IIS. Web sites must have access to ArcGIS Map and Feature services, to the scanning database, and to stored files. The DOT Highway Plans Locator currently requires a direct connection to the scanning activity database. Spatial data is accessed via the ArcGIS service.
4. **File storage** is the service that provides storage for files such as images files produced by scanning operations. Some of the stored files must be available to be served to end users through the web sites. Files are currently stored on files servers running Microsoft Windows.

The goal is to determine a general plan for migrating services and operational activities from GISTC to DOT. This involves the migration of the services mentioned above as well as the scanning operations. Whether or not all services will be migrated and whether there will be overlap in scanning operations between sites will affect the migration process and inter-site connectivity requirements.

Figure 1 shows a diagram of the current operation configuration with data access paths. All servers and services are hosted by the GISTC, and operations occur locally. Connections between services and between operator workstations and server are through the internal WVU network. External access is only available through the DOT Plan Finder and DOT Plan Viewer web sites.



**Figure 1:** Current server and operations configuration.

**Migration Scenarios**

There are several migrations scenarios possible each with their own network connectivity and security considerations. Some of the possible scenarios are presented below. There are **two primary questions** that will drive the determination of which scenario is most appropriate:

1. Will there be simultaneous scanning operations occurring at DOT and at the GISTC?
2. Will any of the services remain at the GISTC? (One possibility being Web Site hosting)

**Scenario 1:**

*All services and operations migrate completely to DOT with no overlap of operations at GISTC.*

In this scenario there is no need for inter-site network connectivity and therefore no special security considerations for on-going operations. All services can be installed at DOT and data can be migrated in bulk using some pre-defined mechanism. A temporary VPN is an option for the data migration or data can be backed up to external hard-drives and hand carried to DOT. The migration of the databases can be done ahead of the final migration in order for DOT staff to test the system and do in-house training. Once the system is validated and final database migration can occur.

In this scenario there is no need to coordinate operations activities between sites.

Figure 2 shows a diagram of the final configuration using this scenario. The configuration is the same as is currently in place at GISTC, simply migrated to DOT. (Note that in this diagram and in others show below the services process may reside on individual servers of may be combined at the discretion of DOT IT)



**Figure 2:** All services and operations located at DOT.

**Scenario 2:**

*Database, ArcGIS, and file services migrate to DOT. Web Site hosting remains at GISTC. All scanning operations migrate completely to DOT with no overlap of operations at GISTC.*

In this scenario the web server at GISTC can access the Feature services and Map services published by the DOT ArcGIS service over the internet without the need for any special network connectivity. Although DOT may want to restrict direct public access to those services. In that case access could be restricted to GISTC only using client certificates.

An access mechanism between the GISTC web server and the files stored at DOT would be required. This could be accomplished using a VPN or other secure connection, or could be accomplished using REST services provided by DOT.

As with the previous scenario, all services can be installed at DOT and data can be migrated in bulk using some pre-defined mechanism. A temporary VPN is an option for the data migration or data can be backed up to external hard-drives and hand carried to DOT. The migration of the databases can be done ahead of the final migration in order for DOT staff to test the system and do in-house training. Once the system is validated and final database migration can occur.

In this scenario there is no need to coordinate operations activities between sites.

Figure 3 shows a diagram of the final configuration using this scenario.



**Figure 3:** Database, ArcGIS, and File Services located at DOT. Web hosting at the GISTC. Scanning at DOT only.

**Scenario 3:**

*This is a variation of either of the two preceding scenarios with the exception that scanning operations will continue to occur at the GISTC concurrently with scanning operations at DOT.*

Concurrent scanning operations introduces two challenges:

1. Coordinating scanning operations.
2. Providing a secure mechanism for GISTC staff to access data stored on DOT file and database servers.

Overcoming the first challenge would require the implementation of new procedures to ensure that no conflict occur when recording scanning activity and when publishing updates to the geodatabase. Developing a new, possibly web-based, operator interface may help facilitate the coordination of activities.

Providing a secure method for accessing file storage and databases would take two forms. The first could be by establishing a VPN connection between sites. This would require the least amount of software development work. The second would be to develop a web-based operator interface and corresponding REST services that would allow access to remote operators over the internet.

Figure 4 shows a diagram a potential configuration using this scenario. Alternatively, a modification of scenario 2, above, could be implemented with a similar insertion of GISTC scanning operations.



**Figure 4:** All services hosted at DOT with scanning operations occurring concurrently at DOT and the GISTC.

**Scenario 4:**

*This scenario used cloud hosted database and file services. This configuration allows operations, web services, and ArcGIS services to reside at both sites simultaneously.*

The challenge of coordinating scanning operations remains as in Scenario 3, however this scenario mitigates the challenge of establishing secure connections for operations work across the two centers. New procedures must still be implemented to ensure that no conflict occur when recording scanning activity and when publishing updates to the geodatabase at two different centers. Developing a new, possibly web-based, operator interface may help facilitate the coordination of activities.

This scenario has the advantage of being able to be implemented while scanning operation continued to take place at the GISTC. The new cloud services can be validated by experienced GISTC staff.

This option would require that DOT own the cloud service accounts. GISTC would be granted access to the services, but administration would be under the direction of DOT.

Figure 5 shows a diagram a potential configuration using this scenario. In this scenario, the Web Server and ArcGIS Server could be housed at either location.

****

**Figure 5:** File and Database services hosted on the Cloud. Web and ArcGIS servers can be located either at DOT and/or the GISTC. Scanning operations occurring concurrently at DOT and the GISTC.

 Document prepared by: Jim Schindling
 2/2/2023