

**Navajo Department of Health**

**Navajo Epidemiology Center**

**RFP Bid No: 22-01-2706KS**

**Cloud Computing and Information Security Services**

Description: The Navajo Epidemiology Center under the Navajo Department of Health is requesting proposals for a Cloud Computing and Information Security Services in Window Rock, AZ.

Contact Person: Tex Etsitty  
Senior Network Specialist  
Phone Number (928) 551-0173  
Email: [tex.etsitty@navajo-nsn.gov](mailto:tex.etsitty@navajo-nsn.gov)  
Fax Number: (928) 871-6255

Deliver to: The Navajo Dept. of Health  
P.O. Box 1390  
Administration Building 2, #2296  
Window Rock Boulevard  
Window Rock, AZ 86515  
Attn: Tex Etsitty, Navajo Epidemiology Center

# Navajo Epidemiology Center

## Cloud Computing and Information Security Services

### 1. ISSUING OFFICE

This Request for Proposal (RFP) is issued by Navajo Epidemiology, Navajo Department of health, Navajo Nation.

### 2. PURPOSE

This RFP provides prospective respondents with sufficient information to enable them to prepare and submit a proposal for consideration.

### 3. SCOPE

This RFP contains the instructions governing the proposal to be submitted and the material to be included therein; mandatory requirements which must be met to be eligible for consideration; and other requirements to be met by each proposal

### 4. SUBMIT DEADLINE:

Proposal(s) must be received by Thursday, **March 3, 2022 at 3:00pm MDT.**

All parties responding to this **RFP Bid No: 22-01-2706KS** are instructed to submit or send four (4) proposals (1 original and 3 copies) to the following address:

Navajo Epidemiology Center, Navajo Department of Health, P.O. Box 1390, Window Rock, Arizona 86515

Courier Service/Deliver to:

Navajo Epidemiology Center, Window Rock Blvd, Administration Building #2 Window Rock, Arizona 86515

All responses to this bid shall be sent in a sealed envelope, including a return address, and clearly marked on the outside of the envelope; the following:

BID #22-01-2706KS  
NEC CLOUD COMPUTING AND INFORMATION SECURITY SERVICES  
DO NOT OPEN-BID PROPOSAL

### 5. REJECTION OF PROPOSALS

Navajo Epidemiology Center reserves the right to reject any and all proposal. The RFP may be canceled at any time and all proposals may be rejected in whole. in part when the Navajo Epidemiology Center Department Staff determines it is in the best interest of the Navajo Nation.

## 6. RESPONSE MATERIAL OWNERSHIP

All material submitted regarding this RFP shall become property of The Navajo Nation and will not be returned to the respondent. Responses received will be retained by Navajo Epidemiology Center and may be reviewed by any person after final selection has been made. Navajo Epidemiology Center has the right to use any or all system ideas presented in reply to this RFP.

## 7. NAVAJO PREFERENCE

Navajo preference will apply to this RFP. Consultants should indicate if they are Navajo Nation Priority One or Two Vendors on their submission packaging.

## 8. SUFFICIENT APPROPRIATION

Any contract awarded as a result of this RFP is contingent upon the appropriation of funds. A contract award may be determined or reduced in scope if sufficient appropriate or authorization does not exist. Such terminations will be effected with written notice to the contractor. The program's decision as to whether sufficient appropriations and authorizations are available will be accepted by the contractor as final.

## 9. TYPE OF CONTRACT

The Navajo Nation will utilize a standard Professional Services Contract for the procurement of goods and services for this project.

## 10. BID OPENING

Due to the pandemic, where possible, the bid opening activities will be conducted via conference call. Please contact Tex Etsitty (contact information above) after the submit deadline to obtain call-in information.

### **Evaluation and Criteria**

1. An evaluation team will judge the proposals received in accordance with the general criteria used herein. The team may request for any additional information that the teams feels necessary.
2. Failure of a respondent to provide any information requested in the RFP may result in disqualification of the proposal. All proposals must be endorsed with the signature of a responsible official having the authority to bind the respondent to the execution of a contract.
3. The sole objective of the review team will be to evaluate and select the respondent who best meets this objective.

#### 4. Evaluation Criteria

Evaluation Criteria	Points
Priority 1 or 2 vendor a) Priority One vendor (10 pts.) b) Priority Two vendor ( 5 pts.) c) Non-Priority vendor ( 0 pts.)	10
Bid Organization a) Typed written on 8-1/2" X 11" paper b) One original bid and 3 copies c) Binding and indexing	10
Letter of Transmittal a) Provide Statements of Qualifications. b) Provide background on company c) Identifying individual(s) as specified above. d) List of similar services provided to other business customers	20
Proposed Workplan a) Provide a detailed and comprehensive description of how the Respondent intends to complete the SOW in this RFP. b) This discussion shall include, but not be limited to items requested in SOW including an overall construction schedule	40
Proposed Cost (Sealed in Separate Envelope) a) The respondent will provide detailed breakdown cost for fees, expenses and advertising.	10
Attachments a) Activity and Project timeline and diagram method b) Provide a sample of the diagram	10
<b>Total Score</b>	100

#### 7. SOVEREIGNTY

The Navajo Nation will not relinquish any of its sovereignty rights

## 1. Background

The Navajo Epidemiology Center (NEC), under the Navajo Dept. of Health (NDOH), serves as a Public Health Authority under the Indian Health Care Improvement Act (IHCIA) for purposes of the Health Insurance Portability and Accountability Act (HIPAA). The Centers for Disease Control and Prevention (CDC) established the Tribal Epidemiology Centers Public Health Infrastructure (TECPHI) cooperative agreement to assist tribes in improving and building the public health infrastructure and capacity of Tribal Epidemiology Centers (TECs). Goals as a TEC and for TECPHI are to develop a data management system involving a baseline establishment on secure data handling with the mission of empowering Diné people to achieve hozhó (harmony) through Naaʼniih Naalkaah (epidemiology). The NEC TECPHI goal is to implement a secure database system to manage relevant data for monitoring health status, maintaining disease surveillance, conducting health research, conducting disease outbreak investigation, reporting health data, providing technical assistance, and identifying priority health concerns for the Navajo People.

Another innovative long-term goal of NEC is Data Sovereignty: to have the Navajo People exercise rights as an Indigenous people to manage, control, and analyze its people's health information and data. This includes access to all databases storing clinical and health information about Navajo people on or off the Navajo Nation. This includes, but not limited to, Indian Health Service, Bureau of Indian Affairs, State Departments, Tribal Health Organizations, Non-governmental Organizations, and private clinics managing and storing data. This would be accomplished by establishing data linkages, data connections, and a Navajo Nation surveillance system to quickly identify critical or reportable infectious diseases.

Currently, data management processes are fragmented as they are ongoing through non-centralized avenues. In order to achieve efficiency in these matters, a centralized or an organized system must be created. Information Systems Security integrity is crucial to establishing this data management system as it will house and store clinical and health data entrusted by the Navajo people.

## 2. Scope

This Statement of Work (SOW) describes the requirements for the cloud computing servers for database, data warehouse, Web hosting, Information Systems Security (ISS) Consultation services, and other consultation services. These services will be executed in congruence with an extensive knowledge of HIPAA, HITECH Act, Data Sharing Agreements, Memorandum of Agreements or Understanding dynamics when applicable. There will be an added consideration for knowledge and innovation encouraging Data Sovereignty.

The following services are considered to be within the scope of the Cloud computing and Information Systems Security (ISS) Consultation services. The services sought will entail data being handled appropriately and securely in every capacity regarding its existing, planned, and emerging practices/infrastructure:

- Sustainable data management plan and related processes
- Server and Information Systems Security training to NEC staff
- Tailor assessments and recommendations to HIPAA, HITECH Act, MoA/MoU and architecture when applicable.

- Data Sharing Agreements (DSA) and Memorandum of Agreements or Understanding (MOA, MOU) standards when applicable
- Perform information and network security risk assessment
- Provide insight and recommendations in the improvement and implementation of a sustainable data management plan and related data processes in software and network development considering technologies (e.g. system, network, mobile, cloud, on-going IT security best practices).
- ISS training to NEC, NDOH and Navajo Nation Department of Information Technology (DIT) staff
- ISS Consultation services
- Highly confidential or sensitive assessment activities will be on-site. All other risk assessments can be performed at the consultant's location.
- The location for on-site services is the Navajo Nation administrative offices area, Window Rock, AZ. Due to COVID-19 safety, work is expected to be done remotely as much as possible. When in-person services are needed, work and knowledge exchange will take place in Window Rock, AZ.
  - It is highly recommended that all consultants coming to the Navajo Nation are fully vaccinated against Covid-19, including a booster, and test negative on a COVID-19 rapid test prior to entering the Navajo Nation. Masks are also required on the Navajo Nation.
  - Provide cost on travel break down
    - Include all travel, living, meals, materials, incidentals, out-of-pocket, and other expenses as part of its price proposal. Provide documentation substantiating the amount of the fixed fee attributable to travel, out-of-pocket and other expenses, including the estimated number of flights, hotel stay nights or other accommodations used to develop the fixed fee.

### 3. Information Security Requirements

#### 3.1 Perform information and network security risk assessment

- 3.1.1 Develop an initial security assessment of agency-wide risks.
- 3.1.2 Provide quantitative and substantive measures, and advice on the security assessment.
- 3.1.3 Levels and depth of a risk assessment are defined by:
  - Information sensitivity
  - Systems and applications exposures
  - The initial level of the perceived risk factors for likelihood and impact
  - Breach response

#### 3.2 Performing information security risk assessments

- 3.2.1 Perform assigned risk assessments of existing Information Systems (IS) environments and data handling practices, as well as proposed changes to these environments and practices.
- 3.2.2 Risk assessments must be led by technical subject matter experts knowledgeable in the current and emerging technical, threat and attack landscape that is relevant to the subject of the assessment. Assessments will be performed through collaboration with in-house subject matter experts as appropriate. This will include the evaluation of DIT's PEN test results (if applicable).

3.2.3 Provide guidance and support for security initiatives in the form of project definition documentation and consult with the in-house staff (NEC IT, or DIT) on project sequencing and tasks as related to the risk of the data management plan.

3.2.4 Results of the risk assessment shall be submitted in standard report form:

3.2.4.1 Full report – includes all assessment raw data, summary data, recommendations, and guidance.

3.2.4.1.1 Recommendations:

- These will allow consistent and standardized processes in which NEC will be able to do a self-assessment after a certain amount of time to compare periodic assessments.
- Data collection, dissemination, transfer, storage, disposition, and archival methodologies in regards to HIPAA and HITECH Act Compliance. This would entail recommendations on hardware/software environments needed to execute compliance in NEC's current infrastructure state, in short-term improvements state, and long-term infrastructure state.
- Webhosting methodologies working in congruence with secure data storage integrity.

3.2.4.1.2 Guidance: Along with recommendations, guidance shall be provided on self-assessments to be conducted.

3.2.4.1.3 Data inventory reporting:

- This will include data sources, data storage, and application usage.

3.3 Information security risk assessment training

3.3.1 The contractor shall provide training, training materials, and coaching on the methodologies and tools to enable participants to understand the process. This training and coaching can be performed remotely.

## 4. Cloud computing servers for database, data warehouse, Web hosting

4.1 IaaS/PaaS Technical Requirements

4.1.1 Server Requirements

4.1.1.2 Database

- CPU 8 Frequency: 2.2GHz and threads :16
- Windows servers 2019 or higher
- Ram 32GB
- 500GB Scalable

4.1.1.3 Data Warehouse

- CPU 8 Frequency: 2.2GHz and threads :16
- Windows servers 2019 or higher
- Ram 32GB
- 500GB Scalable

4.1.1.3 Web hosting

- Microsoft IIS
- Windows servers 2019 or higher

- Storage: 500GB
- Ram: 32gb
- CPU 8 threads :16

#### 4.1.1.4 Storage Systems

- SAN: 500GB Scalable
- Back-Up: 1TB Scalable
- Achieve: 1TB Scalable

### 4.1.2 Applications Requirements

4.1.2.1 Licenses and Subscriptions – Consultant will be responsible for all licensing, hardware and software subscription for applications, OS, servers, databases, etc

4.1.2.1.1 Responsibilities include but are not limited to:

- Database
- Server
- IIS server
- Application

#### 4.1.2.2 Database – MicroSoft Sql server

- Database management
- Database set up
- Database connection to other platforms
- Complete Data Encryption
- Proper Encryption Key Management
- Authentication
- Data sovereignty
- Automatic Updates
- Data Disposal

#### 4.1.2.3 Virtual Machine encryption

- Virtual Machine hardware encryption with a high level of encryption
- Audit Logs
- Access Control
- Unique User IDs
- Authentication
- Server Backups
- Dedicated Infrastructure
- Automatic Updates
- Data Disposal
- Multi-Factor Authentication
- SSL Certificates
- Offsite Backups

#### 4.1.2.4 Web Server- IIS

- Demilitarized zone

4.1.2.5 Backup System and capability – ability to recover and restore the system and data from failure or loss situation

4.1.2.5.1 Recover and restore system and data



- Back up
  - Application
  - Data
  - Webpages, database, environment, connections, IP address
- Back retentions and archiving
  - Length of time of backups
  - Offsite archiving
- Recovery Time objectives
  - Length of time for backup restoration
    - Production of environments
    - Development and test environments
- Recovery Point Objective
  - Max length of Time from backup
- Snapshot capability
  - Snapshot of environment is required (on demand copy of system and data)

4.1.2.6 Scalable Resource – Ability to increase/decrease resources as needed, to support any unpredictable usage.

#### 4.1.2.6.1 Servers

- CPU
- RAM
- Disk Space

#### 4.1.2.6.2 Storage

#### 4.1.2.6.3 Database

#### 4.1.2.6.3 Bandwidth

### 4.1.3 System Usage

- Number of Users: 8-15 users
  - Peak Times of Users: 8:00 am- 5:00 pm (MT)
  - Average Time of Users: 3 hours
- Amount of bandwidth: 20mbs- 30mbs
  - Amount of bandwidth: 2-3 hours average

### 4.1.4 Help Desk Support

- 24x7 365 days
- On call

### 4.1.5 Security

#### 4.1.5.1 HIPAA

#### 4.1.5.2 HITech

#### 4.1.5.3 Vulnerability Scanning and Patching

#### 4.1.5.4 Security Architecture Review

#### 4.1.5.5 Data sovereignty

#### 4.1.5.6 SQL server

- Proper Encryption Key Management
- Authentication

- Data sovereignty
- Automatic Updates
- Data Disposal

#### 4.1.5.7 Virtual Machine encryption

- Virtual Machine hardware encryption with a high level of encryption
- Audit Logs
- Access Control
- Unique User IDs
- Authentication
- Automatic Updates
- Data Disposal
- Multi-Factor Authentication
- SSL Certificates

## 5. Qualifications

5.1 The Contractor shall have a minimum of four years of experience providing the services described in the Statement of Work, with at least two contracts handling instances of HIPAA, HITECH Act, and MoA/MoU experience.

5.2 The Contractor shall have a proven record of at least two satisfied customers to whom the relevant services were provided within the past three years.

5.3 The Contractor shall have knowledge and experience in the following disciplines:

5.3.1 PEN Testing

5.3.2 Systems Engineering

5.3.3 Network Engineering

5.3.4 Vulnerability Testing

5.3.5 Webhosting and data reporting applications

5.3.6 Relational Databases

5.3.7 Minimum, two years of experience

5.3.8 Experience performing and teaching Risk Assessments

## 6. Information Handling

Though not expected frequently, it is imperative sensitive information is properly handled and protected by the Contractor. A Business Associate Agreement will be reached in appropriately handling sensitive information.

## 7. Quality assurance and deliverables

7.1 All interim drafts and working materials shall comply with the provided Agency classification and marking standards.

7.2 NEC will have access to engage and review drafts and working materials when clarification, inquiries, and corrections are appropriate.

7.3 Proposed Network Map for data management plan goals.

7.4 Proposed Dataflow Map for data management plan goals.

## 8. Formal acceptance of deliverables

NEC will formally accept the final deliverables in written notification.

## 9. Deliverables

The Contractor's reporting is to include documentation on the processes, tools, and approaches used to complete the agreed upon task(s). The results will be transparent with explicit language. The results will also be related to the deliverables at the conclusion of the assessments. When applicable, deliverables will reflect NEC's information classification requirements (i.e. HIPAA/HITECH Act/etc. Compliances).

9.1 The Contractor shall deliver the following items:

9.1.1 Risk Assessment Report

9.1.2 Vulnerability Assessment

9.1.3 Provide documentation of setup and network configurations

- Cloud Computing documentation,
- Diagrams of network.

9.1.4 Provide knowledge transfer, functional overviews of implemented products, demonstration of operations, including educational resources to further provide insight into the products' implementation, architecture, and integration,

9.1.5 Best practices guidelines

## 10. NEC Responsibilities

The NEC will have the following responsibilities:

10.1 The NEC will provide idealized data management plan.

10.2 The NEC will provide appropriate and necessary technical information.

10.3 The NEC will provide partner and in-house subject matter experts.

10.4 The NEC will respond to requests for further information, review draft documents, and provide comments.

## Attachment 1 – NEC Information Technology Environment

NEC is setup on the Navajo Nation network managed by Navajo Nation Department of Information Technology (DIT). Currently NEC is on the same network as many other agencies within the Navajo Nation. However, a potential of having its own VLAN within the Navajo domain is being explored.

A1.1 The following devices are managed by DIT:

- Network devices (Routers/switches/etc.)
- Network connections (LAN/WAN/VPN setups/VLAN)
- SharePoint
- Firewalls
- Servers

A1.2 NEC and NNDOH IT staff configure and manage the following devices:

- Desktops, laptops, tablets, cell phones, printers.

A1.3 Estimated DIT Information Technology components to be assessed and evaluated:

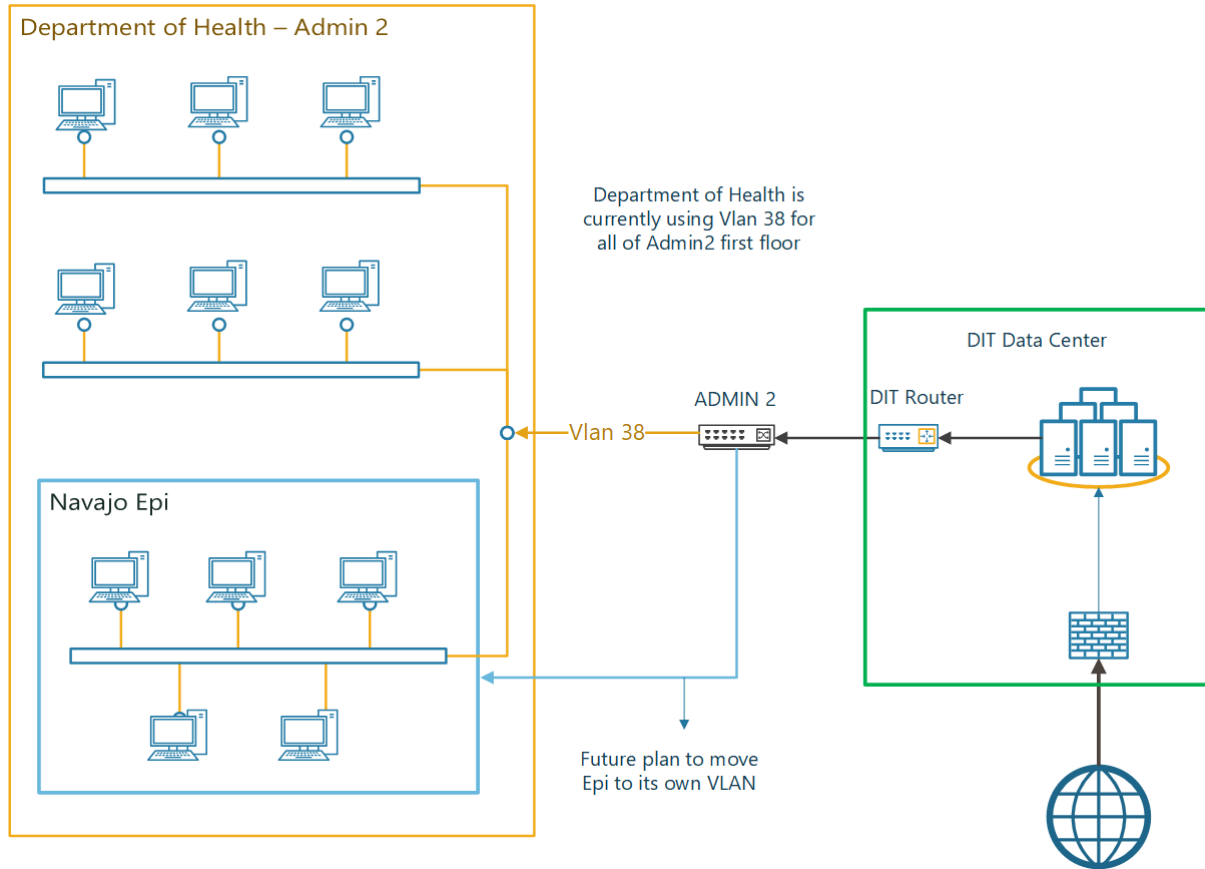
- Number IP Addresses: 3 public (from firewall) and 27 private IP Addresses (LAN)
- Number of Web applications: Public: 2, Private: 0
- Desktops: 80, laptops: 30, Mobile: 50, Network Devices: 50, IoT: VoIP phones: 70
- Geographic Requirements: one place
- Isolated/air gapped zones: 0
- Network
  - Internet: Navajo Nation Network 1gb bandwidth
  - Firewall: Palo Alto Firewall
  - Bandwidth: 100-150 mbs
  - Layer3: Dell switch Vlan 38
- Virtual Private Network
  - VPN: Global Protect
  - VLAN: vlan 210

A1.4 Current NEC Infrastructure

- Server
  - None
  - Standalone PC/MAC – 9 current users, 15-20 user capacity
- File System
  - SharePoint
- Network
  - Internet: Navajo Nation Network 1gb bandwidth
  - Firewall: Palo Alto Firewall
  - Bandwidth: 100-150 mbs
  - Layer3: Dell switch Vlan 38
- Virtual Private Network
  - VPN: Global Protect
  - VLAN: vlan 210

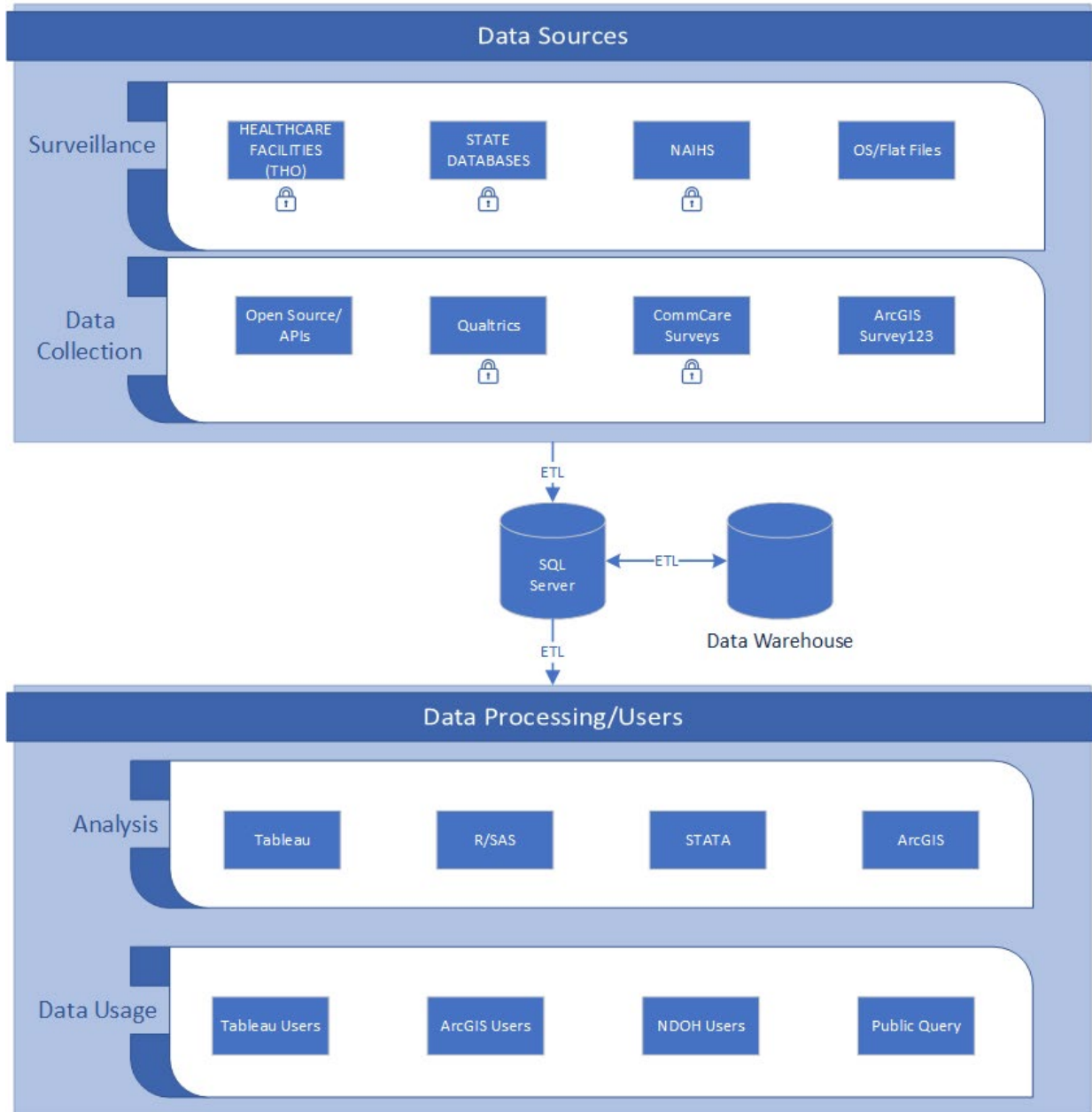
## Attachment 2 – Diagrams for consideration

### A2.1 Network Diagram:



## A2.2 Data Flow Diagram

### Draft Navajo Epidemiology Center Centralized Data Repository and System



Created by Delores Becenti, SPSS 1/12/2022

Regulated

API; Application Programming Interface  
 R; R statistical and graphics language/environment  
 SAS; SAS Analytics Software  
 STATA; STATA Statistical Software  
 THO; Tribal Health Org.  
 NAIHS; Navajo Area Indian Health Service  
 NDOH; Navajo Dept. of Health  
 OS; Operating System  
 ETL; Extract, Transform, Load tools  
 SQL; Structured Query Language

## Definitions:

IaaS- Infrastructure as a service

PaaS- Platform as a Service

BaaS- Backup as a Service

DRaaS - Disaster Recovery as a Service