### Prompt [evaluate for cybersecurity vulnerabilities](https://m365.cloud.microsoft/chat/entity1-d870f6cd-4aa5-4d42-9626-ab690c041429/eyJpZCI6IlZYTmxjbFl4ZkdoMGRIQnpPaTh2YzNWaWMzUnlZWFJsTFdsdWRDNXZabVpwWTJVdVkyOXRMM3hQU1VRNll6SmhNak0zWVRNdE5XVTROeTAwWWpnekxUbG1aamN0T1dKbE56YzFORE5pWmpBemZERTFZVGMwTWpVeUxUbGpOVGN0TkRKa01TMWhNVGd5TFRBMFpHTTBNbU16WVRJMVpYd3lNREkxTFRBM0xURXdWREUyT2pFeU9qUXpMalkwTURJeE5UZGEiLCJzY2VuYXJpbyI6InNoYXJlTGlua1ZpYVBhZ2UiLCJwcm9wZXJ0aWVzIjp7InByb21wdFNvdXJjZSI6InVzZXIiLCJjbGlja1RpbWVzdGFtcCI6IjIwMjUtMDctMTBUMTY6MTI6NDQuMTExWiJ9LCJjaGF0VHlwZSI6IndlYiIsInZlcnNpb24iOjEuMX0)

Based on the content of the NAESB WGQ Quadrant Electronic Delivery Mechanism (QEDM) Version 4.0 standards manual, here is an evaluation of potential cybersecurity vulnerabilities and considerations:

### 🔍 Cybersecurity Vulnerability Evaluation

#### 1. Separation of Cybersecurity Standards

* **Observation**: As of Version 4.0, cybersecurity-related standards have been moved to a separate **NAESB WGQ Cybersecurity Related Standards manual**.
* **Implication**: This separation may lead to **delays in implementation** or **incomplete integration** if implementers do not reference both documents together.
* **Recommendation**: Ensure that all implementers are aware of and comply with the separate cybersecurity manual. Consider integrating critical cybersecurity requirements directly into the QEDM manual or providing cross-references.

#### 2. Authentication Mechanisms

* **Observation**: The document supports **HTTP Basic Authentication** and **Multi-Factor Authentication (MFA)** for Customer Activities Web sites.
* **Vulnerability**: Basic Authentication, even over HTTPS, is considered **less secure** than modern token-based or certificate-based authentication.
* **Recommendation**: Encourage or mandate the use of **MFA** and **OAuth 2.0** or **SAML** for stronger identity assurance.

#### 3. Transport Layer Security (TLS)

* **Observation**: The document mandates the use of **transport layer security (TLS)** for all sensitive communications.
* **Vulnerability**: The document does not specify **minimum TLS versions** or **cipher suite requirements**.
* **Recommendation**: Explicitly require **TLS 1.2 or higher**, and deprecate older versions. Define acceptable cipher suites and key lengths.

#### 4. Firewall and Port Management

* **Observation**: The document recommends minimizing the number of outbound ports and using a limited set of TCP ports.
* **Vulnerability**: If not properly enforced, **open ports** can be exploited for lateral movement or data exfiltration.
* **Recommendation**: Implement **strict firewall rules**, **network segmentation**, and **intrusion detection systems (IDS)** to monitor traffic.

#### 5. Flat File Uploads (Interactive FF/EDM)

* **Observation**: The standard allows for **interactive flat file uploads** via web forms.
* **Vulnerability**: This introduces risks such as:
	+ **File injection**
	+ **Malware upload**
	+ **Improper validation**
* **Recommendation**:
	+ Enforce **file type and content validation**
	+ Use **sandboxing** for file processing
	+ Implement **rate limiting** and **logging** for upload endpoints

#### 6. Client-Side Security

* **Observation**: The document references compatibility with various browsers and plug-ins.
* **Vulnerability**: Use of outdated or unsupported plug-ins (e.g., Adobe Flash, ActiveX) can introduce **client-side vulnerabilities**.
* **Recommendation**: Remove references to deprecated technologies and enforce **modern browser standards** only.

#### 7. Data Retention and Access

* **Observation**: Standards specify retention periods for operational data (e.g., 90 days for notices).
* **Vulnerability**: Improper access controls or lack of encryption for stored data could lead to **data leakage**.
* **Recommendation**:
	+ Encrypt data at rest
	+ Implement **role-based access control (RBAC)**
	+ Audit access logs regularly

#### 8. Change Notification and Testing

* **Observation**: Trading partners must notify others of business rule changes at least two weeks in advance.
* **Vulnerability**: Lack of automated validation or rollback mechanisms could lead to **incompatibility or downtime**.
* **Recommendation**: Use **automated testing frameworks** and **version control** for configuration changes.

### ✅ Strengths Noted

* Emphasis on **open standards** and **interoperability**
* Support for **redundant internet connections** and **topographical diversity**
* Clear delineation of **roles and responsibilities** in data exchange

Would you like a summarized checklist or a risk matrix to help prioritize these findings?