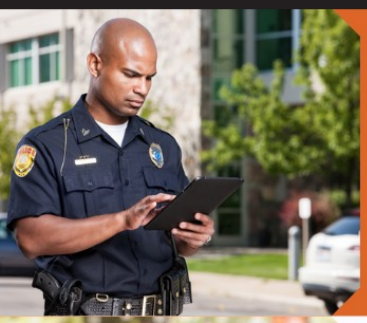
Envoy Data SECURITY

MTRIX® America Inc. [AUTHENTICATION SOLUTIONS]

480-221-3054
www.envoydata.com
cwendt@envoydata.com
Chris Wendt

864-800-3409
www.mtrix.com
dennis.robare@mtrix.com
Dennis Robare

COMPLIANCE MFA MATRIX



CJIS (Criminal Justice Information Services)

- Organizations accessing CJIS must implement MFA on all systems containing CJI.
- MFA is required even in physically secure locations or criminal justice conveyances.
- Failure to comply may result in denial of access to FBI's CJIS resources and data, as well as monetary fines.
- MFA must use at least two factors to authenticate individuals.

PCI DSS (Payment Card Industry Data Security Standard)

- All-access to the Cardholder Data Environment (CDE) must be gated by multi-factor authentication.
- MFA applies to all types of system components, including cloud, hosted systems, and on-premises applications.
- At least two of the three authentication methods (something you know, something you have, something you are) must be used.
- Passwords for accounts used by applications and systems must be changed regularly.
- MFA must not be susceptible to replay attacks.

CMMC (Cybersecurity Maturity Model Certification)

- Only privileged users require MFA for local access. If regular user accounts have administrative rights only on their computers, they are not considered a "privileged account" and as such do not require MFA for local access.
- All users require MFA for network/remote access.

GLBA (The Gramm-Leach-Bliley Act)

- **Written Information Security Program:** Financial institutions must adopt a comprehensive, written program for safeguarding customer information. This program should include administrative, technical, and physical safeguards appropriate to the institution's size, complexity, and the sensitivity of customer data.
- **Designation of a Qualified Individual:** A qualified individual must oversee, implement, and enforce the information security program. This person can be an employee or an outside consultant.
- **MFA Requirement:** Multi-Factor authentication (MFA) must be implemented for systems containing customer information unless an equivalent or stronger control is approved by the qualified individual.

HIPPA (Health Insurance Portability and Accountability Act)

- **Strong Authentication Requirement:** HIPAA's Security Rule requires covered entities to implement procedures for verifying the identity of users seeking access to ePHI. This includes the use of authentication methods that are "reasonable and appropriate".
- **Recommendation of MFA:** MFA is a security best practice for enhancing authentication and access control. The Department of Health and Human Services (HHS), which enforces HIPAA, has issued guidance recommending the use of MFA as part of a comprehensive security program.
- **Flexibility in Implementation:** HIPAA allows covered entities to determine the most appropriate authentication measures based on their specific risk factors, organizational size, complexity, and capabilities. Even though MFA is not explicitly mandated, HIPAA offers organizations the flexibility to choose the authentication methods that best meet their security needs and risk profile; for example, passwords, biometrics, tokens, or MFA.