Identity and Access Management Modernization

An IAM modernization program that centralizes identity management, implements strong authentication, and establishes governance controls, forming the foundation for Zero Trust access decisions.

PRACTICE

Cyber Resilience and Zero Trust

CLIENT PROFILE

Federal agency modernizing identity infrastructure to support multi-factor authentication, conditional access, and identity governance across cloud and on-premises resources

Challenge

- Fragmented identity sources with inconsistent access policies across systems
- Reliance on passwords without enterprise-wide multi-factor authentication
- No centralized identity governance for access reviews, provisioning, and de-provisioning

Approach

- Consolidate identity sources into a unified identity provider with directory synchronization
- Implement phishing-resistant MFA and conditional access policies based on user, device, and context
- Deploy identity governance for automated provisioning, access reviews, and separation of duties
- Integrate identity signals with SIEM for identity-based threat detection

Typical Outcomes

- Unified identity fabric with consistent policy enforcement across all resources
- Elimination of password-only access and reduced credential-based attack risk
- Automated access lifecycle management with auditable governance controls

Procurement Paths

- GSA MAS for IAM engineering and professional services
- NASA SEWP V and SEWP VI for identity platform licensing
- CIO-CS (NITAAC) for enterprise identity solutions

Compare vehicles and ordering steps on **How to buy**.

Partner Technology Examples

- Microsoft Entra
- CrowdStrike
- Palo Alto Networks
- Fortinet

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.