TAG

ADVISORY REPORT

FEDERAL REQUIREMENTS FOR SECURING HYBRID IDENTITY

FIVE EYES ALLIANCE GUIDANCE

DR. EDWARD AMOROSO,
FOUNDER & CEO, TAG
RESEARCH PROFESSOR, NYU

ADVISORY REPORT

FEDERAL REQUIREMENTS FOR SECURING HYBRID IDENTITY

FIVE EYES ALLIANCE GUIDANCE

DR. EDWARD AMOROSO,
FOUNDER & CEO,
TAG, RESEARCH PROFESSOR, NYU

This report provides an overview of the security-related functional requirements, including mandates, that exist for U.S. Federal Agencies operating hybrid Active Directory and Entra ID identities.

INTRODUCTION

Hybrid identity in the context of Microsoft Active Directory (AD) and Entra ID involves integration of an organization's on premises and cloud-based identity systems. It allows organizations, including U.S. Federal Agencies, to bridge the gap between their traditional perimeter-protected infrastructure and modern public cloud services such as Azure. The goal is to enable management and cybersecurity across both types of environments.

On premises-hosted AD has long been the backbone of enterprise identity management in the public sector, providing authentication, authorization, and directory services within an agency's network, often protected by a trusted network interconnect (TIC). With cloud computing, however, Entra ID (formerly Azure AD) emerged to facilitate access to applications such as Microsoft 365 and other SaaS platforms. Hybrid identity allows these systems to coexist securely.

Some agencies use tools such as Entra Connect to synchronize accounts, passwords, and other identity data between locally hosted and Entra ID. This creates a single source of truth for users accessing hybrid resources, and enables use of a single set of credentials, thanks to features like Single Sign-On (SSO). In fact, uniform identity management is a primary objective to streamline workflows and apply policies such as multifactor authentication (MFA) usage.

That said, implementing hybrid identity is not without challenges, especially in cybersecurity. For example, misconfigurations of AD or inconsistent identity policies between hybrid environments can create severe vulnerabilities. Cybersecurity agencies from the Five Eyes alliance, including the Cybersecurity Infrastructure and Security Agencies (CISA) and the National Security Agency (NSA), urged organizations to strengthen security controls for AD, a prime target for cyber attackers, in a report that highlights more than a dozen tactics used by threat actors to exploit AD. The report, "Detecting and Mitigating Active Directory Compromises," offers guidance on protective measures, including using free tools such as Semperis' Purple Knight AD security assessment tool to find and fix vulnerabilities.

Because of the security vulnerabilities of hybrid AD systems, requirements, many in the form of federal mandates, have emerged that focus on addressing these security weaknesses in hybrid identity environments. Below, we provide an overview of these important functional demands.

U.S. FEDERAL MANDATES FOR HYBRID IDENTITY SECURITY

As suggested above, securing hybrid identity systems for AD is critical for U.S. Federal Agencies to maintain operational integrity and avoid incidents. While many agencies do adhere to broader cybersecurity frameworks, addressing identity-specific requirements and leveraging advanced tools can enhance their defensive posture. Below is an outline of three specific U.S. federal mandates designed to improve hybrid identity security:[1]

1. **Executive Order (EO) 14028:** Improving the Nation's Cybersecurity – This EO dictates that agencies must adopt zero trust, which includes securing identity systems. They must implement MFA across critical systems, including hybrid, and they must encrypt sensitive data at rest and in transit, ensuring hybrid AD tasks such as replication are secure.

2. **Federal Information Security Modernization Act (FISMA);** Agencies must assess and mitigate risks associated with identity compromise including AD recovery and secure administration.[2] This requirement involves enforcing stringent identity access management (IAM) controls for privileged accounts within AD.

3. **OMB Memorandum M-22-09:** Moving the U.S. Government Towards Zero Trust Cybersecurity Principles – This important memorandum from the Office of Management and Budget (OMB) requires agencies to ensure robust identity federation and secure hybrid AD integrations with cloud providers like Azure AD.

FUNCTIONAL REQUIREMENTS FOR HYBRID IDENTITY SECURITY

Complementing these works are additional mandates in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF 2.0), NIST 800-53 requirements, NIST 800-63 Digital Identity Guidelines, Continuous Diagnostics and Mitigation (CDM), and Cybersecurity and Infrastructure Security (CISA) Binding Operational Directives (e.g., BOD 22-01). A sampling of the most important mandated requirements (listed alphabetically) is shown below.

1. **Active Directory Hardening:** Agencies must regularly mitigate misconfigurations, such as weak Group Policy Object (GPO) permissions or unsecured LDAP connections.

2. **Backup and Recovery Requirements:** Agencies must implement immutable backups of AD databases including AD recovery playbooks for ransomware or domain compromises.

---

[1] *Readers are warned that as U.S. Presidential Administrations change, the corresponding Federal mandates – especially in the form of Executive Orders – are prone to change. The list generated here was created during late 4Q2024 as the U.S. prepares for a new Administration in 2025.*

[2] *The leadership team from commercial cybersecurity vendor Semperis (**https://www.semperis.com/**) was particularly helpful in the technical discussions surrounding development of this analyst report. Our observation at TAG is that Semperis is an excellent choice for a U.S. Federal Agency to partner with to address a plethora of the mandated functional capabilities listed here.*

3. **Behavioral Anomaly Detection:** Agencies must deploy solutions to detect deviations in user behavior indicative of account compromise within hybrid AD environments.

4. **Conditional Access Policies:** Agencies must enforce policies that assess the security posture of devices accessing hybrid AD systems, as outlined in zero trust guidelines.

5. **Continuous Monitoring:** Agencies are required to use Continuous Diagnostics and Mitigation (CDM) tools for monitoring AD system configurations and compliance.

6. **Endpoint Detection and Response (EDR) Integration:** Agencies must monitor hybrid identity systems for anomalous activity and lateral movement using AD logs.

7. **Event Logging and SIEM Integration:** Agencies must enforce logging for all authentication and authorization within hybrid AD systems (as required by EO 14028).

8. **Hybrid Identity Integration:** Agencies should strengthen integration points between on-premises AD and cloud identity systems, addressing gaps in synchronization and security.

9. **Identity Threat Detection:** Agencies must implement specialized tools like Microsoft Defender for Identity to detect and respond to potential breaches in AD environments.

10. **Patch Management:** Agencies must enforce regular patching of AD domain controllers and ensure hybrid AD environments are up to date against known vulnerabilities.

11. **Privileged Access Management (PAM):** Agencies must periodically rotate and store privileged credentials in AD, including just-in-time (JIT) access for administrative tasks.

12. **Red and Purple Team Exercises:** Agencies must conduct regular simulated attacks to test the resilience of hybrid identity systems and identify gaps in existing security measures.

13. **Secure Trust Relationships:** Agencies must mandate security reviews of forest and domain trust configurations to ensure secure delegation of authentication.

While many federal agencies meet generic mandates like defense-in-depth and backup requirements, securing hybrid identity systems like Active Directory demands specific and enhanced measures. By adhering to federal directives, implementing advanced security tools, and continuously monitoring identity systems, agencies can achieve a stronger security posture that aligns with evolving threats and compliance requirements.

NEXT STEPS

U.S. Federal Agencies are advised to select excellent partners to assist in determining the optimal solutions to address their mandated requirements across hybrid identity for AD. As suggested above, vendors such as Semperis will complement important controls from Microsoft, and our experience is that working with vendors such as Semperis will reduce operation and planning risk.

In addition, our research and advisory team at TAG is always available to assist U.S. Federal Agencies with their hybrid identity planning. Existing federal TAG customers can access assistance through their TAG Research as a Service (RaaS) portal, and newer customers can access these services through contracts with key value-added resellers such as Carahsoft. We hope to hear from you.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence.