INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-15 19:03 UTC

White House Cyber Official Highlights Identity Security as Critical Defense Against AI-Enabled Threats

GOVERNANCE | MEDIUM

SCC Item ID	SCC-GOV-2026-0036
Type	Governance
Severity	MEDIUM
Affected Products	Federal IT infrastructure (general); identity and access management systems
Published	2026-05-14
Discovery Source	Gemini

Executive Summary

A White House cybersecurity official signaled that identity security, zero trust architecture, privileged access controls, and multi-factor authentication is the federal government's primary defense layer against AI-enabled threats. The statement reflects existing mandates under OMB M-22-09 and the National Cybersecurity Strategy, but carries renewed urgency as AI lowers the cost and sophistication bar for credential-based attacks. Federal agencies and organizations aligned with federal supply chains should treat this as a policy signal to accelerate identity program maturity reviews.

Technical Analysis

This item is a strategic policy signal, not a vulnerability disclosure. No CVE, CVSS score, or active exploit is associated. The statement maps directly to three MITRE ATT&CK techniques: T1621 (Multi-Factor Authentication Request Generation), T1078 (Valid Accounts), and T1556 (Modify Authentication Process). The core threat model is that AI-augmented adversaries, using tools that automate credential stuffing, MFA fatigue attacks, and identity enumeration, still require authenticated access to move laterally or persist. Strong identity controls interrupt that requirement regardless of how the initial access was obtained. Relevant federal mandates include OMB M-22-09 (Federal Zero Trust Strategy, requiring phishing-resistant MFA and device-level trust by FY2024 milestones) and the 2023 National Cybersecurity Strategy. The June 2025 White House executive order sustaining cybersecurity efforts reinforces these requirements. No patch action is applicable; this is a control posture item.

Action Checklist

1. Audit current MFA coverage: identify any privileged accounts, service accounts, or internet-facing applications not enrolled in phishing-resistant MFA (FIDO2/WebAuthn). Prioritize accounts with access to sensitive data or administrative functions.
2. Review identity logs for T1621 and T1078 indicators: query your SIEM for MFA push fatigue patterns (multiple rapid MFA requests from a single account), anomalous login times, and logins from unexpected geographies or ASNs. Use authentication logs from your IdP (Entra ID, Okta, Ping) as the primary source.
3. Validate privileged access controls: confirm that privileged access workstations (PAWs) or equivalent segmentation are in place for admin accounts. Audit for standing privileged access that should be converted to just-in-time (JIT) access.
4. Map your zero trust implementation against OMB M-22-09 milestones: verify device trust enforcement, micro-segmentation status, and whether phishing-resistant MFA is deployed at all identity perimeters. Document gaps with remediation timelines.
5. Update identity-related detection rules: ensure your SIEM or XDR has active detection for T1556 (authentication process modification), including alerts on changes to MFA configurations, conditional access policies, and directory authentication settings.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal/compliance if SIEM queries reveal confirmed MFA bypass events (Entra ID ResultType 50074/500121 without corresponding user-acknowledged push), any Conditional Access or MFA configuration changes not tied to a change management ticket, or if the organization is a federal agency or federal contractor subject to OMB M-22-09 and FedRAMP authorization — these findings constitute potential reportable incidents under FISMA and may trigger CISA reporting obligations within 1 hour of confirmed compromise.
Recovery Notes	After remediating MFA gaps and converting standing privileged access to JIT, monitor Entra ID Sign-In Logs and Okta System Log continuously for 30 days for recurrence of T1621 fatigue patterns and any re-emergence of accounts accessing resources without phishing-resistant MFA — AI-enabled adversaries will retry against the same identity perimeter once initial access is blocked. Verify that all Conditional Access policy changes made during remediation are reflected in the Entra ID audit log with expected actor UPNs, and confirm no new service principals or app registrations were silently created during the exposure window (query `Get-MgServicePrincipal -All | Where-Object {$_.CreatedDateTime -gt (Get-Date).AddDays(-90)}`). Validate recovery completeness by re-running the CISA ScubaGear assessment and confirming all previously red-rated OMB M-22-09 identity pillar controls have moved to green before declaring the remediation closed.

Forensic Artifacts	Entra ID Sign-In Logs (full JSON export) — fields `mfaDetail`, `conditionalAccessStatus`, `riskLevelAggregated`, `ipAddress`, and `location` expose AI-driven credential spray and MFA fatigue patterns specific to T1621; retain for minimum 90 days per AU-11 (Audit Record Retention) | Okta System Log events for `user.mfa.attempt_bypass`, `user.mfa.factor.deactivate`, and `system.policy.update` — these are the exact event types written when an adversary abuses push fatigue (T1621) or silently disables MFA controls (T1556) within an Okta-managed identity perimeter | Entra ID Audit Log entries for `category eq 'Policy'` and `operationName contains 'authentication method'` or `operationName contains 'Conditional Access'` — captures T1556 authentication process modification attempts where a compromised privileged account alters phishing-resistant MFA enforcement to re-enable weaker factors | Active Directory Security Event Log Event ID 4672 (Special Logon) and Event ID 4624 (Logon Type 3 — Network) from domain controllers — establishes which privileged accounts exercised standing admin rights during the exposure window, supporting reconstruction of lateral movement following AI-assisted credential compromise under T1078 | Entra ID Service Principal and App Registration creation log (`Get-MgAuditLogDirectoryAudit -Filter "activityDisplayName eq 'Add service principal'"` for the past 90 days) — AI-enabled adversaries frequently persist by creating OAuth app registrations with delegated MFA bypass permissions after initial identity perimeter compromise, leaving this artifact as the primary persistence indicator

Per-Action IR Details

Audit current MFA coverage: identify any privileged accounts, service accounts, or internet-facing applications not enrolled in phishing-resistant MFA (FIDO2/WebAuthn). Prioritize accounts with access to sensitive data or administrative functions.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing identity security posture and access controls before AI-enabled credential attacks are attempted

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Export all accounts and MFA enrollment status using free IdP reporting: in Entra ID, run `Get-MgUser -All | Select UserPrincipalName, StrongAuthenticationMethods` via Microsoft Graph PowerShell (free); in Okta, use the Admin Console System Log or free Okta API (`GET /api/v1/users?filter=status eq "ACTIVE"` cross-referenced with `GET /api/v1/users/{id}/factors`). Flag any global admin, service principal, or app registration lacking FIDO2 enrollment. A 2-person team can script this in under 4 hours using PowerShell or Python with the free Microsoft Graph SDK.

Evidence: Before remediating MFA gaps, capture a point-in-time snapshot of: Entra ID Sign-In Logs (portal.azure.com > Azure AD > Sign-in logs, export to CSV) filtered for `authenticationRequirement eq 'singleFactorAuthentication'`; Okta System Log entries with `eventType eq 'user.authentication.sso'` and `outcome.reason` containing 'MFA not required'; and the full list of Conditional Access policy exclusions (Entra ID > Security > Conditional Access > Named Locations and excluded users). This establishes the pre-remediation attack surface baseline if a breach is later discovered.

Review identity logs for T1621 and T1078 indicators: query your SIEM for MFA push fatigue patterns (multiple rapid MFA requests from a single account), anomalous login times, and logins from unexpected geographies or ASNs. Use authentication logs from your IdP (Entra ID, Okta, Ping) as the primary source.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlating IdP authentication events to identify MITRE T1621 (MFA Request Generation) and T1078 (Valid Accounts) abuse patterns consistent with AI-assisted credential attacks

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query IdP logs directly: in Entra ID, use Log Analytics (free tier) with KQL — `SigninLogs | where ResultType == '50074' or ResultType == '500121' | summarize count() by UserPrincipalName, bin(TimeGenerated, 5m) | where count_ > 5` to detect MFA fatigue bursts; in Okta, filter System Log via API for `eventType eq 'user.mfa.attempt_bypass'` or `user.authentication.auth_via_mfa` with `outcome.result eq 'FAILURE'` more than 3 times in 10 minutes per user. Use the free Sigma rule `proc_creation_win_mfa_push_fatigue.yml` (SigmaHQ GitHub) converted to native log query syntax for on-premises environments. A 2-person team can run these queries manually on a daily schedule using cron + Python.

Evidence: Collect and preserve before analysis: Entra ID Sign-In Logs for the past 30 days with full JSON export including `conditionalAccessStatus`, `mfaDetail`, `ipAddress`, `location`, and `riskLevelAggregated` fields — these fields specifically expose AI-driven spray patterns and VPN/proxy ASN anomalies; Okta System Log entries for `user.session.start` and `user.mfa.attempt_bypass` events with actor IP and geolocation; ASN ownership records for observed login IPs (query via `whois` or free APIs such as ipinfo.io) to identify hosting providers commonly used for AI-driven credential stuffing infrastructure; and any existing Conditional Access policy named location exclusions that may have been silently modified (T1556 precursor).

Validate privileged access controls: confirm that privileged access workstations (PAWs) or equivalent segmentation are in place for admin accounts. Audit for standing privileged access that should be converted to just-in-time (JIT) access.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: reducing the blast radius of AI-enabled credential compromise by eliminating standing privileged access and enforcing PAW segmentation before adversaries pivot from compromised identities

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), NIST IA-2 (Identification and Authentication — Organizational Users), NIST IR-4 (Incident Handling), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without PIM/PAM tooling: in Entra ID, enable Microsoft Entra Privileged Identity Management (PIM) free tier to convert Global Administrator and other high-privilege roles to eligible (JIT) rather than permanent assignments — run `Get-MgRoleManagementDirectoryRoleAssignment -Filter "assignmentType eq 'Assigned'"` to enumerate all standing privileged assignments. For PAW enforcement without dedicated hardware, enforce a Conditional Access policy (free in Entra ID P1) restricting admin portal access to compliant, Entra-joined devices only. On-premises environments can use free Group Policy to restrict `BUILTIN\Administrators` logon rights to named admin workstations via `User Rights Assignment > Deny log on locally`.

Evidence: Before converting standing access to JIT, capture: Entra ID role assignment export including `assignedDateTime`, `directoryScopeId`, and `principalId` for all permanent role members (preserves pre-change audit trail); Windows Security Event Log Event ID 4672 (Special Logon — privileges assigned at logon) from domain controllers, exported for the past 90 days, to establish baseline of which accounts have been exercising standing admin rights; and Active Directory `AdminSDHolder` group membership (`Get-ADGroupMember -Identity 'Domain Admins' -Recursive`) to identify any accounts added by potential adversary activity consistent with T1078 (Valid Accounts) persistence under OMB M-22-09 identity perimeter assumptions.

Map your zero trust implementation against OMB M-22-09 milestones: verify device trust enforcement, micro-segmentation status, and whether phishing-resistant MFA is deployed at all identity perimeters. Document gaps with remediation timelines.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: using the threat signal from White House identity security guidance and AI-enabled attack escalation to drive structured zero trust gap analysis and compliance posture improvement against OMB M-22-09 mandates

Controls: NIST CA-7 (Continuous Monitoring), NIST CA-2 (Control Assessments), NIST IA-5 (Authenticator Management), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a

Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a GRC platform: download the free CISA Zero Trust Maturity Model v2.0 self-assessment spreadsheet (cisa.gov/zero-trust-maturity-model) and map each OMB M-22-09 milestone (phishing-resistant MFA at all identity perimeters, device compliance signals, encrypted DNS) against current state using a simple RAG (Red/Amber/Green) worksheet. Use the free CISA SCuBA M365 Secure Configuration Baseline assessment scripts (github.com/cisagov/ScubaGear) to automatically evaluate Entra ID and Microsoft 365 configurations against federal baseline — ScubaGear runs via PowerShell and produces an HTML gap report with no licensing cost. Document findings in a remediation register with 30/60/90-day timelines.

Evidence: Before conducting the gap assessment, preserve current state artifacts: Conditional Access policy export from Entra ID (Settings > Export) and Okta policy configuration snapshots — these establish the pre-assessment baseline and serve as evidence if a breach is later attributed to a documented gap; CISA SCubaGear baseline report output (JSON and HTML) timestamped at assessment date; and device compliance report from Entra ID (`Get-MgDeviceManagementManagedDevice` or Intune compliance dashboard export) showing percentage of devices with trusted posture enforcement — critical for OMB M-22-09 device pillar compliance documentation.

Update identity-related detection rules: ensure your SIEM or XDR has active detection for T1556 (authentication process modification), including alerts on changes to MFA configurations, conditional access policies, and directory authentication settings.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: deploying threat-specific detection capability for T1556 authentication process tampering before AI-enabled adversaries use compromised privileged credentials to silently disable phishing-resistant MFA controls

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-4 (Incident Handling), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a commercial SIEM: configure Entra ID Diagnostic Settings to stream Audit Logs to a free Log Analytics workspace and alert on `operationName eq 'Update Conditional Access policy'` or `operationName eq 'Update authentication method policy'` — these are the exact log entries written when an adversary disables FIDO2 or modifies CA policy post-compromise. In Okta, enable free System Log streaming and alert on `system.policy.update` and `user.mfa.factor.deactivate` event types. For on-premises Active Directory, deploy the free Sysmon configuration (SwiftOnSecurity/sysmon-config) and monitor Windows Security Event ID 4719 (System audit policy changed) and Event ID 4706 (New trust created to domain) from domain controllers — these fire when an adversary modifies Kerberos or NTLM authentication settings consistent with T1556. Use the free Sigma rule `win_security_mfa_config_change.yml` from SigmaHQ for cross-platform translation.

Evidence: Before updating detection rules, capture the current rule inventory and any existing alert history: export all active SIEM/XDR detection rules related to authentication (search for rule names containing 'MFA', 'Conditional Access', 'authentication', 'directory') to establish a before-state for audit purposes; pull Entra ID Audit Log entries for `category eq 'Policy'` covering the past 90 days to check whether any MFA or CA policy changes occurred prior to rule deployment — a T1556 adversary operating in a pre-detection window would appear here; and export Okta System Log for `eventType sw 'system.policy'` for the same period to identify any unauthorized policy modifications that existing rules would have missed.

Detection Guidance

Focus detection on the three mapped ATT&CK techniques. For T1621 (MFA fatigue): alert on five or more MFA push requests within a 10-minute window for a single account; correlate with login failures preceding the push sequence. For T1078 (Valid Accounts): monitor for logins outside business hours, impossible travel events, and first-time access to sensitive resources by established accounts. For T1556 (Modify Authentication Process): alert on any changes to MFA enrollment, conditional access policy modifications, or directory service authentication configuration changes, particularly those made outside change management windows. Log

sources: IdP audit logs (Entra ID sign-in and audit logs, Okta System Log), Active Directory Security event log (Event IDs 4624, 4625, 4648, 4723, 4724, 4738), and VPN/SSO access logs. Behavioral baseline: flag deviations from per-user login patterns using UEBA if available.

Framework Mappings

MITRE-ATTACK

- **T1621** — Multi-Factor Authentication Request Generation
- **T1078** — Valid Accounts
- **T1556** — Modify Authentication Process

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access

Sources

Source	URL	Tier
5. National Cybersecurity Strategy Good Practice - NCS Guide 2025	https://ncsguide.org/ncs-guide-2025/5-national-cybersecurity-strate...	T3
Sustaining Select Efforts to Strengthen the Nation's Cybersecurity ...	https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-...	T1

Source	URL	Tier
[PDF] National Cyber Security Strategy Guidelines | CCDCOE	https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf	T3
Breaking Down the New National Cybersecurity Strategy - YouTube	https://www.youtube.com/watch?v=EarH8BdsPNM	T3
[PDF] NATIONAL CYBERSECURITY STRATEGY - Biden White House	https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/Nat...	T1

Generated 2026-05-15 19:03 UTC by TJS Security Command Center