INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-07 15:07 UTC

DHS Confirms Breach of Homeland Security Information Network (HSIN)

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0216
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Homeland Security Information Network (HSIN), associated SharePoint collaboration system
Published	2026-07-06
Discovery Source	Gemini

Executive Summary

DHS has confirmed it is investigating a cyberattack against the Homeland Security Information Network (HSIN), a classified collaboration platform used by federal, state, local, and private-sector security partners. The intrusion, reported to have occurred between late May and early June 2026, also targeted a connected SharePoint system; data exfiltration has not been confirmed and no threat actor has been attributed. The primary business risk is potential exposure of sensitive operational planning content, including material related to 2026 FIFA World Cup security coordination, which could compromise event security posture and interagency trust.

Technical Analysis

According to secondary reporting from Security Boulevard and MSN/Reuters, the HSIN intrusion involved unauthorized access to a sensitive SharePoint-based collaboration environment. No CVE or CWE identifiers apply; HSIN breach is a platform compromise, not a software vulnerability. MITRE ATT&CK techniques associated with this incident pattern include T1213 (Data from Information Repositories), T1078 (Valid Accounts), and T1530 (Data from Cloud Storage Object). The attack vector and initial access method have not been publicly disclosed by DHS. No official DHS advisory, CISA alert, or US-CERT technical bulletin with scope or exfiltration confirmation has been identified in available sources. Confidence in breach confirmation is medium: secondary outlets report DHS has confirmed the intrusion, but no first-party technical statement has been identified to corroborate attack method, affected data types, or remediation status.

Action Checklist

1. Step 1: Containment, If your organization has HSIN access, immediately review active sessions and revoke credentials for any accounts not actively required. Per NIST AC-2 (Account Management), disable accounts pending re-validation and notify your HSIN point of contact. Isolate any local systems used to access HSIN from broader network segments.
2. Step 2: Detection, Audit authentication logs for HSIN-connected accounts, focusing on the late May through early June 2026 window. Per NIST AU-6 (Audit Record Review, Analysis, and Reporting), review for anomalous access patterns including off-hours logins, access from unfamiliar IP ranges, and bulk document access consistent with T1213 and T1530 behavior. Check SharePoint audit logs for mass download or export activity (per CIS 8.2, Collect Audit Logs). No specific IOC patterns have been disclosed in available source material.
3. Step 3: Eradication, Per NIST AC-17 (Remote Access) and NIST IA-4 (Credential Management), rotate all credentials used to access HSIN and connected SharePoint environments. Remove any third-party or service account access that cannot be immediately validated. No specific patch or vendor advisory has been identified in available source material; await official DHS or CISA guidance before broader remediation.
4. Step 4: Recovery, Validate that only authorized accounts retain HSIN access, per NIST AC-2 and CIS 5.3 (Disable Dormant Accounts). Monitor resumed access sessions for anomalous behavior. Confirm SharePoint access control lists reflect least privilege, per NIST AC-6 (Least Privilege) and CIS 3.3 (Configure Data Access Control Lists). Await official DHS advisory before certifying remediation complete.
5. Step 5: Post-Incident, Conduct a post-incident review of access governance for sensitive collaboration platforms. Map control gaps against NIST AC-5 (Separation of Duties) and NIST AC-6 (Least Privilege). Evaluate whether multi-factor authentication (MFA) and user account permission controls are enforced for all HSIN-connected access points. Per CIS 6.3 (Require MFA for Externally-Exposed Applications), confirm MFA is enforced on all external collaboration system access.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior leadership, legal counsel, and your agency ISSO if any HSIN-connected account shows confirmed unauthorized authentication events during the 2026-05-20 to 2026-06-10 window, if exfiltration of operationally sensitive or PII-containing documents is identified in SharePoint audit logs, or if your organization lacks the internal capability to execute credential rotation and ACL review within 24 hours.
Recovery Notes	Do not certify remediation complete until official DHS or CISA guidance has been issued and reviewed against your specific HSIN configuration, as the root compromise vector has not been publicly confirmed. After re-enabling HSIN access, maintain enhanced monitoring of all HSIN-connected accounts for a minimum of 30 days — specifically watching for off-hours SharePoint access, bulk file operations, and authentication from new source IPs that were not present in the pre-incident baseline. Any newly issued credentials or service account tokens should be tracked in your identity inventory with a mandatory review checkpoint at 15 and 30 days post-recovery.

Forensic Artifacts	SharePoint Online Unified Audit Log (Operations: FileDownloaded, FileSyncDownloadedFull, FileAccessed, SearchQueryPerformed) for the HSIN-connected tenant, covering 2026-05-20 through 2026-06-10 — primary evidence source for data staging or bulk exfiltration consistent with this breach | Azure AD / Entra ID sign-in logs for all accounts assigned to the HSIN application registration, including source IP, user agent, authentication method, and conditional access outcome — key for identifying unauthorized authentication sessions during the breach window | Windows Security Event Log Event ID 4624 (Successful Logon), 4648 (Logon with Explicit Credentials), and 4634 (Logoff) on endpoints used to access HSIN, preserving the local session record independent of the cloud identity logs | Browser profile data (cookies, session storage, download history) from endpoints used for HSIN/SharePoint access — specifically Edge or Chrome profiles at '%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\' — which may contain session tokens or evidence of bulk file downloads saved to local disk | OAuth 2.0 refresh token grant history and service principal permission grants for any third-party or service account integrations with the HSIN SharePoint environment, exported before credential rotation, to identify whether an application-level credential was the initial access vector

Per-Action IR Details

Step 1: Containment — If your organization has HSIN access, immediately review active sessions and revoke credentials for any accounts not actively required. Per NIST AC-2 (Account Management), disable accounts pending re-validation and notify your HSIN point of contact. Isolate any local systems used to access HSIN from broader network segments.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 6.2 (Establish an Access Revoking Process)

Compensating: On Windows endpoints used to access HSIN, run 'query session /server:' to enumerate active RDP and interactive sessions, then 'logoff ' to forcibly terminate. Export active network connections via 'Get-NetTCPConnection | Where-Object {$_.RemoteAddress -match ""} | Export-Csv active_hsin_sessions.csv' before revoking. Use Windows Firewall ('netsh advfirewall firewall add rule name="Block HSIN" dir=out action=block remoteip=') to isolate the local workstation without full network removal.

Evidence: BEFORE revoking credentials or isolating the host, capture: (1) active authenticated sessions against HSIN/SharePoint — export browser session cookies and OAuth tokens from memory using a tool such as SharpDPAPI or by copying the browser profile directory (e.g., '%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Cookies' and 'Network\Cookies' for Edge-based HSIN access); (2) live network connections via 'netstat -ano' or 'Get-NetTCPConnection' filtered to HSIN IP ranges, saved to timestamped file; (3) running process list with parent PIDs ('Get-Process | Select-Object Id,ProcessName,Path,StartTime | Export-Csv') to identify any persistence mechanism launched from the HSIN session context; (4) Windows Security Event Log entries for Event ID 4624 (Logon) and 4648 (Explicit Credential Logon) for the HSIN service account or user accounts, covering the late May–early June 2026 window.

Step 2: Detection — Audit authentication logs for HSIN-connected accounts, focusing on the late May through early June 2026 window. Per NIST AU-6 (Audit Record Review, Analysis, and Reporting), review for anomalous access patterns including off-hours logins, access from unfamiliar IP ranges, and bulk document access consistent with T1213 and T1530 behavior. Check SharePoint audit logs for mass download or export activity (per CIS 8.2 — Collect Audit Logs). No specific IOC patterns have been disclosed in available source material.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query SharePoint Unified Audit Log exports directly via PowerShell: 'Search-UnifiedAuditLog -StartDate 2026-05-20 -EndDate 2026-06-10 -RecordType SharePointFileOperation -Operations FileDownloaded,FileSyncDownloadedFull | Export-Csv hsin_sharepoint_audit.csv'. Filter for accounts downloading more than 20 files in a single session or accessing document libraries outside their normal operational role. For Azure AD / Entra ID authentication logs, use 'Get-MgAuditLogSignIn' filtered by the HSIN application registration ID and date range. Cross-reference source IP addresses against known organizational egress ranges using a free GeoIP lookup (e.g., MaxMind GeoLite2 via 'mmdbinspect').

Evidence: The detection phase itself must capture and preserve log evidence before any log rotation or retention window closes. Immediately archive: (1) SharePoint Online Unified Audit Log for the HSIN-associated tenant, specifically 'FileDownloaded', 'FileSyncDownloadedFull', 'FileAccessed', and 'SearchQueryPerformed' operations between 2026-05-20 and 2026-06-10; (2) Azure AD / Entra ID sign-in logs for all accounts with HSIN application access — export raw JSON via 'Get-MgAuditLogSignIn -Filter "appDisplayName eq \'HSIN\'"'; (3) Windows Security Event Log Event ID 4776 (NTLM authentication) and 4769 (Kerberos ticket request) on domain controllers, if HSIN is integrated with on-premises AD; (4) local browser history and download folder listings on endpoints used for HSIN access, which may reveal bulk file saves consistent with data staging. Note: no confirmed IOC hashes or C2 infrastructure have been disclosed; analysis must rely on behavioral anomalies rather than signature matching.

Step 3: Eradication — Per NIST AC-17 (Remote Access) and D3-CRO (Credential Rotation), rotate all credentials used to access HSIN and connected SharePoint environments. Remove any third-party or service account access that cannot be immediately validated. No specific patch or vendor advisory has been identified in available source material; await official DHS or CISA guidance before broader remediation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST AC-17 (Remote Access), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords)

Compensating: Enumerate all service accounts and third-party application registrations with HSIN or connected SharePoint API access using 'Get-MgServicePrincipal | Where-Object {$_.AppRoles -match "HSIN"}' (or equivalent Graph API call). For each, revoke OAuth refresh tokens via 'Revoke-MgUserSignInSession -UserId ' and reset passwords using the AD 'Set-ADAccountPassword' cmdlet with '-Reset' flag. Document every revoked account in a timestamped CSV before removal to support post-incident review. If PKI certificates were used for HSIN authentication, revoke affected certificates in your CA console (Microsoft CA: 'certutil -revoke ') and publish a new CRL immediately.

Evidence: BEFORE rotating credentials, capture: (1) a full export of all current OAuth token grants and refresh token lifetimes for HSIN-connected application registrations — 'Get-MgUserOauth2PermissionGrant' per affected user; (2) a list of all API permissions currently delegated to third-party applications integrated with the HSIN SharePoint environment; (3) Kerberos TGT and service ticket cache on any on-premises systems using HSIN SSO ('klist' output saved to file), since credential rotation will invalidate these and the cached state is forensic evidence of what was authenticated and when; (4) Windows Credential Manager entries ('cmdkey /list') and browser saved credential stores on HSIN workstations, which may contain stored HSIN credentials the attacker could have harvested. This evidence must be preserved before rotation destroys the baseline credential state.

Step 4: Recovery — Validate that only authorized accounts retain HSIN access, per NIST AC-2 and CIS 5.3 (Disable Dormant Accounts). Monitor resumed access sessions for anomalous behavior. Confirm SharePoint access control lists reflect least privilege, per NIST AC-6 (Least Privilege) and CIS 3.3 (Configure Data Access Control Lists). Await official DHS advisory before certifying remediation complete.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), CIS 5.3 (Disable Dormant Accounts), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Re-validate each HSIN account against your current personnel roster before re-enabling. Use 'Search-UnifiedAuditLog -Operations UserLoggedIn -StartDate ' to baseline first post-recovery logins and compare source IPs against your approved organizational egress ranges. For SharePoint ACL review without enterprise tooling, export site permissions via 'Get-PnPGroupMembership' (PnP PowerShell, free) for every HSIN-connected SharePoint site collection, then diff against your last known-good permissions snapshot. Flag any accounts inactive for more than 45 days per CIS 5.3 and disable immediately.

Evidence: Recovery actions (re-enabling accounts, restoring SharePoint ACLs) alter the system state established during containment. Before modifying ACLs or re-activating accounts, preserve: (1) the current SharePoint site-level permission report as a baseline ('Get-PnPSiteCollectionAdmin' and 'Get-PnPGroupMembership' export) to document the post-containment ACL state; (2) the disabled account list with timestamps from your identity provider, confirming the containment posture before recovery begins; (3) any anomalous sign-in events generated during the containment window, which may indicate attacker attempts to re-authenticate using cached or secondary credentials — query Entra ID sign-in logs for failed authentications against disabled HSIN accounts during the containment period.

Step 5: Post-Incident — Conduct a post-incident review of access governance for sensitive collaboration platforms. Map control gaps against NIST AC-5 (Separation of Duties) and NIST AC-6 (Least Privilege). Evaluate whether D3-MFA (Multi-factor Authentication) and D3-UAP (User Account Permissions) controls are enforced for all HSIN-connected access points. Per CIS 6.3 (Require MFA for Externally-Exposed Applications), confirm MFA is enforced on all external collaboration system access.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Produce a lessons-learned report within 5 business days per NIST 800-61r3 §4. For MFA gap assessment on HSIN-connected access points without enterprise tooling: query Entra ID Conditional Access policies via 'Get-MgIdentityConditionalAccessPolicy' and identify any policy that exempts HSIN or SharePoint application sign-ins from MFA — document each gap with the policy ID, excluded user/group, and application. For separation of duties review, map HSIN user roles against SharePoint permission levels and flag any accounts holding both 'Site Owner' (admin) and 'Member' (contributor) roles on sensitive document libraries, which violates AC-5. Submit findings to your HSIN point of contact and track remediation against CISA's forthcoming advisory.

Evidence: The post-incident phase requires evidence to support lessons learned and future detection improvements. Consolidate and preserve: (1) the complete timeline of HSIN authentication events from 2026-05-20 through the end of containment, as a permanent incident record; (2) the ACL diff reports generated during recovery, documenting the delta between pre-incident, post-breach, and post-remediation SharePoint permission states; (3) all account disable/enable timestamps from the identity provider, supporting a chain-of-custody record for access governance decisions; (4) any DHS or CISA advisories released during or after the incident, which may disclose IOCs or attack techniques that should be retroactively hunted against your preserved log archive.

Detection Guidance

No specific IOCs, event IDs, or technical indicators have been disclosed in available source material. Detection should focus on the techniques mapped to this incident. For T1213 (Data from Information Repositories) and T1530 (Data from Cloud Storage Object): query SharePoint and collaboration platform audit logs for bulk document access, export, or download activity, particularly during the late May to early June 2026 window. For T1078 (Valid Accounts): review authentication logs for logins from unfamiliar geographic locations, unusual hours, or with atypical user-agent strings. Per NIST AU-6, conduct structured review of audit records for these patterns. Per CIS 8.2, confirm audit logging was active and complete for HSIN-connected systems during the reported intrusion window. Per local account monitoring practices, analyze local and federated accounts with

HSIN access for signs of unauthorized use. Until DHS or CISA releases technical indicators, organizations should treat absence of anomalies as inconclusive rather than as confirmation of clean status.

Framework Mappings

MITRE-ATTACK

- **T1213** — Data from Information Repositories
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1213	Data from Information Repositories	Collection
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Homeland Security Information Network (HSIN)	https://www.dhs.gov/homeland-security-information-network-hsin	T1

Source	URL	Tier
DHS Confirms Hackers Breached HSIN Information-Sharing Platform	https://securityboulevard.com/2026/07/dhs-confirms-hackers-breached...	T3
DHS HSIN Breach Threatens World Cup Security - Gblock	https://www.gblock.app/articles/dhs-hsin-breach-world-cup-security	T3

Generated 2026-07-07 15:07 UTC by TJS Security Command Center