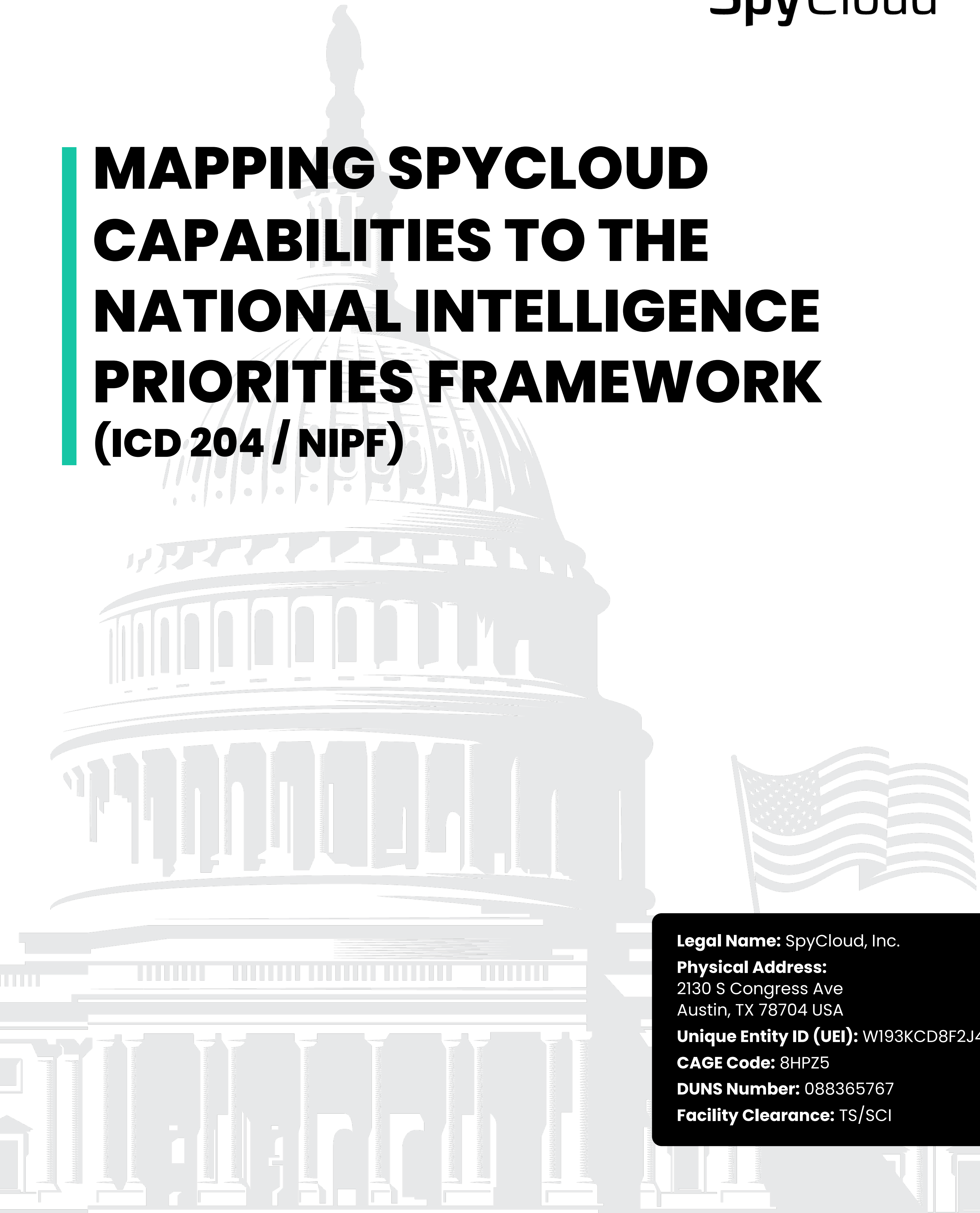
SpyCloud

MAPPING SPYCLOUD CAPABILITIES TO THE NATIONAL INTELLIGENCE PRIORITIES FRAMEWORK (ICD 204 / NIPF)



Legal Name: SpyCloud, Inc.

Physical Address:
2130 S Congress Ave
Austin, TX 78704 USA

Unique Entity ID (UEI): W193KCD8F2J4

CAGE Code: 8HPZ5

DUNS Number: 088365767

Facility Clearance: TS/SCI

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Intelligence Priorities Framework (NIPF), governed by Intelligence Community Directive (ICD) 204, aligns intelligence collection, analysis, and resources to the most critical national security needs. As defined in ICD 204, the NIPF is designed to translate priority intelligence needs into action and evaluate Intelligence Community (IC) responsiveness and performance.

SpyCloud's identity intelligence – powered by data recaptured from breaches, malware-infected devices, phishing infrastructure, and closed criminal communities – adds a unique lens to this framework, translating individual-level identity exposures into enterprise-scale indicators of access governance, cyber maturity, and organizational stress . By curating dark net telemetry and applying advanced identity analytics, SpyCloud enables ODNI to deliver risk-informed, performance-evaluated intelligence judgments aligned to NIPF priorities.

SPYCLOUD INTELLIGENCE OVERVIEW

Source Coverage

- Breach data; malware-exfiltrated identity data including application credentials and session artifacts; successfully phished identity data; and combolists recaptured from the criminal underground
- Data curated, de-duplicated, and normalized for analytic consumption, accessible via SaaS portal, APIs, and integrations

Why It Matters to ODNI

- Converts fragmented identity artifacts into organizational indicators (credential hygiene, session integrity, third-party exposure)
- Supports longitudinal, population-level analysis with rapid time-to-insight enabled by identity analytics and AI-powered finished intelligence
- Delivers evidence-of-compromise (e.g., plaintext passwords, valid session cookies, infection telemetry) to inform strategic warning and counterintelligence

Data Provenance

SpyCloud continuously recaptures identity artifacts from third-party breach files, malware logs, phishing kits, and underground communities of actors. Artifacts are cleansed, correlated, and linked to form holistic identities using proprietary identity analytics technology (IDLink) to reduce noise, resolve duplication, and minimize false positives.

Analyst Consumption

Findings are available through a secure SaaS console, exportable reports, and APIs. Data integrates with SIEM, SOAR, TIP, and identity platforms, enabling incorporation into existing IC analytic and operational workflows.

ALIGNMENT TO NATIONAL INTELLIGENCE PRIORITIES

The following sections are organized by National Intelligence Priorities Framework (NIPF) priority area, with each priority directly mapped to SpyCloud capabilities and indicators that support ODNI's mission to assess risk, readiness, and adversary capacity in accordance with ICD 204.

NIPF Priority:
Foreign Adversaries and State-Aligned Organizations

Intelligence Question

How do foreign governments, militaries, and state-aligned enterprises structure and govern digital access across their ecosystems?

SpyCloud Capability

SpyCloud provides population-level visibility into access governance across ministries, state-owned enterprises (SOEs), contractors, and suppliers by correlating breach-derived and malware-sourced identity artifacts into organizational intelligence.

WHAT SPYCLOUD REVEALS

- Password reuse and reliance on legacy authentication at scale
- Shared or inherited administrative credentials across government and quasi-state entities
- Credential and session overlap between official systems, SSO providers, and commercial supply chains

OPERATIONAL INDICATORS

- Recurrent plaintext or weak credentials associated with official domains
- IDLink-correlated reuse of privileged accounts across multiple state-aligned entities
- Malware-infected hosts tied to government agencies or strategic suppliers

Intelligence Outcome

Enables benchmarking of state cyber maturity, exposes policy-to-practice gaps, and identifies systemic access risks across foreign state ecosystems.

NIPF Priority:
Cyber Threats to Critical Infrastructure and Strategic Sectors

Intelligence Question

Where do identity and access weaknesses create systemic risk across critical infrastructure and strategic industries?

SpyCloud Capability

SpyCloud aggregates identity-centric exposure data across sectors to reveal shared dependencies, privilege concentration, and access patterns that create single points of failure.

WHAT SPYCLOUD REVEALS

- Sector-wide patterns of privileged credential exposure and session theft
- Dependence on shared MSPs, identity providers, and remote-access portals
- Malware infections tied to operational and support environments

OPERATIONAL INDICATORS

- Concentration administrative credentials linked to shared service providers
- Long-lived cookies or tokens associated with OT and infrastructure support portals
- Infection telemetry from endpoints accessing operator systems

Intelligence Outcome

Identifies sector-level identity vulnerabilities exploitable during crisis or escalation and informs infrastructure risk assessments.

NIPF Priority:
Strategic Warning and Organizational Readiness

Intelligence Question

How do changes in identity exposure signal organizational stress, mobilization, or degraded controls?

SpyCloud Capability

SpyCloud supports early warning by tracking short-term and longitudinal changes in credential hygiene, session exposure, and malware activity at the organizational level.

WHAT SPYCLOUD REVEALS

- Shifts in credential exposure during surge, mobilization, or restructuring
- Increased malware-sourced artifacts tied to the same organization
- Expansion of password reuse across personal and professional personas

OPERATIONAL INDICATORS

- Short-interval spikes in exposed credentials for a target organization
- Growth in infected hosts associated with organizational domains
- Elevated reuse of credentials across multiple services

Intelligence Outcome

Provides leading indicators of organizational strain, reduced controls, or heightened operational tempo.

NIPF Priority:
Counterintelligence and Organizational Risk

Intelligence Question

Where do institutional access practices increase susceptibility to foreign intelligence exploitation?

SpyCloud Capability

SpyCloud identifies structural access weaknesses by revealing persistent credential reuse, privileged session exposure, and third-party access paths into sensitive systems.

WHAT SPYCLOUD REVEALS

- Roles and functions with disproportionate exposure
- Recurrent shared or inherited privileged credentials
- Valid session artifacts enabling access persistence or MFA bypass

OPERATIONAL INDICATORS

- Privileged credentials recurring across multiple breach datasets
- Cookies or tokens associated with high-value roles
- Vendor or contractor identities with access to crown-jewel systems

Intelligence Outcome

Supports identification of high-risk functions and institutional CI vulnerabilities beyond individual insider cases.

NIPF Priority:
Transnational and Illicit Organizations

Intelligence Question

How do illicit and transnational networks structure digital access to support coordination, finance, and operations?

SpyCloud Capability

SpyCloud exposes access patterns within illicit organizations by correlating credentials, infections, and accounts across marketplaces, forums, and services.

WHAT SPYCLOUD REVEALS

- Centralized versus compartmented credential models
- Cross-functional reuse across logistics, finance, and communications
- Overlap between cybercrime services and broader illicit activity

OPERATIONAL INDICATORS

- Shared accounts spanning financial and communications platforms
- Infection clusters linking operators across forums and marketplaces

Intelligence Outcome

Illuminates command-and-control structures, dependencies, and organizational choke points.

NIPF Priority:
Intelligence Integration and Organizational Comparison

Intelligence Question

How do adversary organizations compare in cyber maturity, access discipline, and adaptive behavior over time?

SpyCloud Capability

SpyCloud enables comparative and longitudinal analysis by aggregating identity-centric indicators at the organizational and sector level.

WHAT SPYCLOUD REVEALS

- Relative cyber maturity across adversaries and industries
- Evolution of access practices in response to pressure or exposure
- Structural tolerance for persistent identity compromise

OPERATIONAL INDICATORS

- Organization-level scorecards for credential hygiene and privilege concentration
- Trendlines showing improvement or degradation over time

Intelligence Outcome

Improves Improves analytic confidence in judgments of adversary intent, capability, and resilience while supporting enterprise-wide intelligence integration.

DATA TO DECISIONS: ANALYTIC WORKFLOWS FOR THE IC

- **Rapid Scoping:** Start from a single selector (email, domain, IP, phone, password) to surface identity graphs and infrastructure linkages
- **Exposure Triage:** Use AI Insights to prioritize high-risk identities and export finished intelligence
- **Comparative Assessment:** Build organization-level scorecards aligned to NIPF priorities
- **Strategic Warning:** Monitor changes in exposure and infection telemetry as leading indicators of stress

DELIVERY, INTEGRATIONS, AND GOVERNANCE

- **Delivery:** SaaS console, APIs, and on-premise deployment options; exportable analytic products
- **Integrations:** Native integration with SIEM, SOAR, TIP, and identity platforms
- **Governance:** Curated and normalized data; no reliance on customer data for AI model training; customer validation prior to action

BOTTOM LINE

SpyCloud elevates identity telemetry from individual artifacts to institutional intelligence – revealing how adversary organizations structure access, where privilege is concentrated, and when controls degrade under stress. By delivering curated darknet telemetry, advanced linking analytics, and finished intelligence outputs, SpyCloud directly supports NIPF's mandate for risk-informed, priority-aligned assessment of adversary capacity, readiness, and systemic vulnerability.

MAPPING SPYCLOUD IDENTITY INTELLIGENCE TO NIPF PRIORITIES & KEY INTELLIGENCE QUESTIONS

PRIORITY AREA	SPYCLOUD CAPABILITY	INTELLIGENCE OUTCOME
Foreign Adversaries and State-Aligned Terror Groups How do adversary governments manage identity and access?	↘ Recurrent weak credentials that tie foreign state accounts to malware ↘ Cross-entity reuse of privileged accounts ↘ Infected hosts linked to state affiliates and suppliers	Reveal systemic weaknesses and deviations from declared cyber policies
Cyber Threats to Critical Infrastructure and Strategic Sectors Where are critical sectors vulnerable to cyber threats?	↘ Concentration of admin credentials at shared MSP/IDP accounts ↘ Long-lived operational tech sessions (cookies/tokens) ↘ Infection telemetry tied to OT-operator portals	Expose structural indicators of sector-wide identity vulnerabilities
Strategic Warning and Organizational Readiness When are adversary organizations at their most vulnerable?	↘ Short-interval increases in exposed credentials for a single org ↘ Growth in infected hosts linked to org domains ↘ Elevated password reuse across personal and professional personas	Indicate strained security controls during surge or reorganization
Counterintelligence and Organizational Risk Where are access weaknesses creating CI risk?	↘ Recurring privileged credentials across multiple breaches ↘ Cookies/tokens enabling MFA bypass for high-level roles ↘ Third-party exposure to sensitive organizational systems	Identify institutional vulnerabilities and access control failures
Transnational and Illicit Organizations How do transnational illicit groups share access?	↘ Shared accounts spanning money, comms, logistics ↘ Infection clusters linking cybercriminal operators	Illuminate network overlap and command-and-control dependencies
Intelligence Integration and Organizational Comparison How do adversary groups compare over time?	↘ Relative cyber maturity across adversaries and industries ↘ Longitudinal analysis of identity hygiene and access discipline	Benchmark adversary cyber maturity to refine structural judgements

ABOUT SPYCLOUD

SpyCloud is the largest supplier of global identity intelligence sourced from info stealer logs, phished data, combo lists, and third-party breaches. With over a trillion recaptured identity assets and unique records from China, Iran and Russia, SpyCloud reveals previously unknown exposures of companies, people, supply chains, and global relationships to support both OCO and DCO mission outcomes. SpyCloud customers include more than 15 Federal agencies and are certified by USCYBERCOM.