CREATORGAURD

Evaluation Package

Identity-bound authorization and provenance infrastructure for AI and digital media ecosystems.

Document type	Institutional Evaluation Package
Version	1.0
Issued	June 01, 2026
Patent status	Patent Pending — USPTO Docket 85498 · Filed January 28, 2026
SAM.gov UEI	QPGEMXLRHSK5
DUNS	14-464-9875
Schema endpoint	creatorguard.tech/contexts/provenance/v1.json
Primary signal	AI Training Authorization State (machine-readable)
Credential format	W3C Verifiable Credential / JSON-LD / Ed25519Signature2020
Contact	contact@creatorguard.tech

The Problem

Every day, images, music, videos, written works, and other creative content are copied, reposted, and reused across the internet without the knowledge or consent of the original creator. AI companies scrape this content to train models. Social platforms allow reposting without attribution. Bad actors monetize content that does not belong to them. And the original creator has no machine-readable record they can point to that proves they created it first and did not authorize its use.

Unauthorized content use at scale

Images, music, video, and writing are copied and reposted across platforms without permission or compensation to the original creator. The original owner often does not know it is happening until the content has already been viewed or monetized millions of times.

AI training without authorization

AI companies ingest massive datasets of creative content to train models. Currently there is no machine-readable signal at content origin that tells an AI ingestion pipeline whether training is authorized or not. This creates billions of dollars in legal exposure — Getty Images claimed $1.8B in damages from Stability AI. The New York Times is suing OpenAI for similar reasons.

No verifiable origin record

When a dispute arises over who created something first, or whether content was authorized for a specific use, there is no cryptographically verifiable record that proves origin, identity, and authorization state at the time the content was first published. Courts, compliance teams, and platforms have no machine-readable evidence to act on.

$1.8B	Billions	Zero
Getty v. Stability AI claimed damages	In active AI training copyright litigation	Machine-readable authorization standards currently deployed

The CreatorGuard Approach

CreatorGuard establishes a cryptographically verifiable record at content origin. When a creator registers their work, the system binds the content to their verified identity, evaluates it against a governance policy, and produces a machine-readable W3C Verifiable Credential containing the authorization state. This credential travels with the content and can be verified offline by any downstream system — an AI ingestion pipeline, a platform compliance tool, a legal team conducting discovery — without calling CreatorGuard servers.

Four-layer architecture

Layer 1 — Base C2PA provenance stack

Asset binding, manifest stores, cryptographic signatures, hard and soft binding. CreatorGuard builds on top of the existing C2PA standard rather than replacing it. This means platforms already invested in C2PA can add CreatorGuard as an extension layer without re-engineering their existing infrastructure.

Layer 2 — CreatorGuard identity binding

Multi-modal biometric verification anchors the content creation event to a verified creator identity using a W3C Decentralized Identifier (DID). Works for individual creators, enterprises, government entities, and organizations. Identity binding survives platform migration — it is not tied to a username or email that can change.

Layer 3 — CreatorGuard authorization state

Six governance dimensions evaluated at issuance: AI training authorization, commercial reuse permissions, attribution requirements, jurisdictional frameworks, synthetic media disclosure, and derivative works permissions. Each dimension resolves to a machine-readable state. The primary signal — authorizationState.ai_training.authorized — is binary: authorized or not authorized.

Layer 4 — Application and licensing

Field-of-use licensing enforcement, rights clearance, smart contract governance, automated takedown workflows, and audit-ready output records. This is the layer where enterprise legal and compliance teams operate and where licensing revenue is generated.

Primary governance signal

Signal	Field path	Type	Value
AI Training Auth	authorizationState.ai_training.authorized	bool	true / false
Commercial Reuse	authorizationState.commercial_reuse.permitted	bool	true / false

Attribution	authorizationState.attribution.required	bool	true / false
Jurisdiction	authorizationState.jurisdictional.frameworks	array	DMCA / GDPR / etc.
Synthetic Media	authorizationState.synthetic_media.flagged	bool	true / false
Policy Complete	governanceConfidenceScore	float	0.0 – 1.0

Why Existing Solutions Fail

Capability	Copyright law	Watermarks	C2PA	CreatorGuard
Survives platform transit	Partial	No	Partial	Yes
Machine-readable output	No	No	Partial	W3C JSON-LD
AI training authorization	No	No	No	Primary signal
Identity binding	No	No	Voluntary	Cryptographic
Offline verifiable	No	No	Partial	Yes
Legal / audit ready	Manual	No	Partial	Yes
Scales across platforms	No	No	Limited	Yes

Enterprise outcomes

For content platforms and stock media companies

A machine-readable record that proves what content is authorized for AI training ingestion. Platforms can demonstrate to regulators and in litigation that they have a verifiable authorization layer — transforming their compliance position from reactive to defensible. Target organizations: Getty Images, Shutterstock, Associated Press, Reuters.

For AI training pipeline operators

A credential they can check before ingesting content that provides documented evidence of authorization state at time of ingestion. This converts 'we didn't know this content was unauthorized' from a legal defense into a verifiable compliance record. Target organizations: OpenAI, Google DeepMind, Stability AI, enterprise AI pipeline operators.

For social platforms and content distributors

A provenance layer that identifies original creators, flags unauthorized reposts, and provides the audit trail needed to enforce rights claims and compensate original creators. Target organizations: YouTube, Meta, TikTok, X, music streaming platforms.

For government and regulated industries

SAM.gov registered. Eligible for federal procurement today. Applicable to synthetic media detection mandates, chain-of-custody requirements for digital evidence, and AI governance compliance frameworks under the EU AI Act and emerging US synthetic media legislation.

Licensing and Access

CreatorGuard IP is available for licensing under structured terms. Two licensing tracks are available corresponding to the two sides of the authorization infrastructure network.

Track	Issuance licensing	Consumption licensing
Who	Content platforms, stock media, creator registries	AI training operators, platforms, enterprise legal tools
What	License to issue CreatorGuard credentials on content assets	License to consume and verify CreatorGuard credentials
Value	Compliance layer, brand safety, rights monetization	Training data authorization, audit trail, liability reduction
Examples	Getty, Shutterstock, AP, music platforms, publishers	OpenAI, Google, Adobe, enterprise AI pipeline operators
Structure	Field-of-use license, per-credential or enterprise flat	Per-ingestion-check or enterprise infrastructure license

Institutional registration

SAM.gov UEI	QPGEMXLRHSK5
DUNS	14-464-9875
USPTO Docket	85498 — Multi-Modal Content Authentication and Authorization Platform
Priority date	January 28, 2026
Inventors	Eddie Evans, Jerry Joseph
Patent counsel	Law Office of Jerry Joseph, PLC · (202) 570-4009
Website	creatorguard.tech
Schema endpoint	creatorguard.tech/contexts/provenance/v1.json
Contact	contact@creatorguard.tech

Request Access Under NDA

Licensing discussions, acquisition review, full integration documentation, and technical evaluation materials are available to qualified institutional parties under NDA. Requests reviewed within 5 business days.

Submit request at: creatorguard.tech/access
Direct contact: contact@creatorguard.tech