PROTECTING NATIONAL SECURITY SYSTEMS (NSS) DATA

Closing the File Integrity Gap in Modern NSS Architectures with VeraFile

Abstract v1.2

This paper addresses a persistent integrity risk in National Security Systems, where mission-critical data cannot be reliably validated once it leaves trusted system boundaries. It introduces VeraFile as a lightweight, infrastructure-independent mechanism that ensures every file remains tamper-evident and independently verifiable at the point of use - regardless of system, environment, or control boundary.

VeraSec Technologies

About VeraSec Technologies LLC

VeraSec Technologies is a pioneer in Artifact Identity Security *(AIS)*, focused on moving the security context from the infrastructure directly to the file itself. While traditional security models rely on centralized systems to establish and maintain trust, VeraSec's patent-pending VeraFile technology empowers files to carry their own verifiable identity - preparing them for an actual Zero Trust world.

Operating at the forefront of Portable File Identity *(PFI)* technology, VeraSec invented the Validation Integrity Key *(VIK)* process. This innovation patches a fundamental vulnerability in traditional PKI that has persisted for decades. By cryptographically binding a file's content and metadata into a compact, human-readable identifier embedded directly within the artifact, VeraFile helps organizations set up durable, portable trust in every digital asset, signed or un-signed - wherever it travels.

About The Publisher

Brian Hajost (bhajost@verasec.net) is a cybersecurity entrepreneur and technologist with more than 30 years of experience in information security, compliance automation, and trusted computing systems.

As the founder of SteelCloud, he pioneered the automation of DISA STIG and CIS benchmark compliance for the DoD, federal agencies, and enterprise customers. Brian holds 15 patents in information technology and mobile security. In 2022 he was named one of the *"Top 10 Most Influential People in Cyber Security"* by CIO Views.

His current work focuses on solving what he describes as the Artifact Identity Problem - the absence of durable identity for files as they move across distributed infrastructures and untrusted networks.

Disclosure

The statistics, file distribution percentages, and PKI adoption rates presented in this document represent generalized industry and government estimates based on publicly available data. These metrics are provided for illustrative purposes. Individual federal and DIB environments will exhibit variance based on specific mission architecture and internal IT policies.

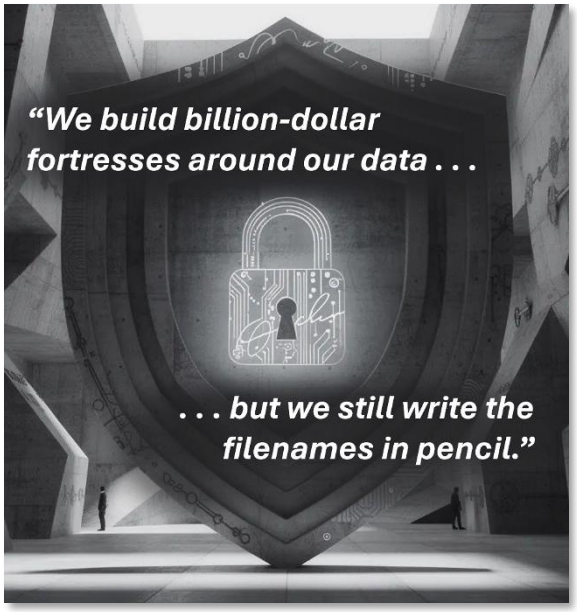
Protecting National Security Systems Data Starts with the File Itself

Closing the File Integrity Gap in Modern NSS Architectures with VeraFile

Executive Summary

Within National Security Systems *(NSS)*, integrity is not a secondary control or compliance objective - it is the foundational condition that determines whether data can be trusted, decisions can be made, and missions can be executed with confidence. Every log file, intelligence report, targeting dataset, and operational artifact must retain its authenticity across time, systems, and environments, often long after it has left the infrastructure in which it was created.

Despite this mandate, modern NSS architectures fail to ensure files remain trustworthy once they move beyond controlled boundaries. Instead, they rely on a model where trust is anchored in systems, identities, and infrastructure, assuming files simply inherit that trust. In practice, they do not.



Despite decades of investment in cryptographic controls, monitoring systems, and Zero Trust initiatives, a critical vulnerability persists: files themselves remain untrusted. They move across domains, classifications, and coalition environments without carrying durable, independent proof of integrity. Existing mechanisms, particularly PKI-based signing, are inconsistently applied, operationally burdensome, and often absent at scale.

This paper argues that the integrity gap in NSS is not a failure of cryptography or Zero Trust strategy - it is a failure of architectural focus. Integrity has never been bound directly to the file itself.

VeraFile introduces a fundamentally different model:

- ***Every file carries its own cryptographic proof of integrity - independent of systems, infrastructure, or chain of custody.***

This establishes a portable, infrastructure-independent trust layer that aligns with the operational realities of national defense environments, introducing a new architectural standard: Portable File Identity *(PFI)*.

The Structural Integrity Gap in NSS Architectures

National Security Systems were originally designed around controlled environments. Trust was established through system accreditation, identity enforcement, and network boundaries; data within those systems was implicitly trusted because the systems themselves were secured.

That assumption no longer holds.

Operational data now moves continuously across domains, classification levels, coalition networks, and disconnected environments. Files are exported, transmitted, copied, transformed, and re-ingested into systems that were never part of their original trust boundary. At each transition point, the chain of custody weakens, and eventually, it disappears entirely. What remains is the file itself - detached from its originating system and stripped of the context that once validated it.

Existing integrity controls do not survive this transition:

- **Access controls** are lost when files leave their originating systems.
- **Metadata** is frequently altered or discarded.
- **Monitoring systems** cannot extend beyond their specific environments.
- **Cryptographic protections**, even when present, are rarely applied consistently across the full spectrum of operational data.

As a result, NSS environments routinely process files whose integrity is assumed but not verified. This is not a theoretical concern; it is a daily operational reality.

The PKI Reality: *Limited Penetration, Limited Protection*

The federal government has long relied on Public Key Infrastructure (PKI) as the authoritative mechanism for data authenticity and integrity. In controlled use cases - identity authentication, secure communications, and formal document execution, PKI is both necessary and highly effective. However, its practical application at the file level within NSS is severely limited.

Data Type	% of Files	PKI Coverage
Logs & Machine Data	35 – 45%	<1%
Office Files / CUI	20 – 30%	<2%
Backups & Archives	15 – 20%	<1%
PDFs	10 – 15%	5 – 10%
Software / Scripts	5 – 10%	40 – 60%

Across defense environments, PKI is pervasive at the identity and transport layers but sparsely applied at the data artifact layer. The operational reality is consistent across agencies: the vast majority of files *(typically >95%)*, particularly high-volume operational data, are not digitally signed.

The limitations of PKI at the file level include:

- **Impractical Volume:** Logs, configuration exports, intelligence extracts, and system-generated artifacts are produced at velocities that render traditional PKI signing workflows impossible. In high-volume telemetry pipelines, signing approaches zero.
- **Computational Overhead:** Traditional PKI validation requires external certificate chains and infrastructure that bottleneck data streams. Testing confirms that, depending on file size and an organization's PKI infrastructure performance, VeraFile will validate files 10x to 20x faster than PKI, making artifact-level integrity practical at scale.
- **Disproportionate Protection:** Signing is typically reserved for finalized presentation documents rather than the work-in-process data that underpins critical analysis and mission execution.
- **Contextual Vulnerability:** Signatures often bind only to portions of file content and exclude the filename from the cryptographic boundary. Consequently, a file's contextual identity - how it is named, interpreted, and acted upon, remains unprotected.
- **Discrete Validation:** Signature verification is rarely automated at scale and is almost never enforced continuously. Validation occurs at discrete points, leaving extended windows where modified files can move undetected.

Most files move through national security environments unsigned, unverified, and implicitly trusted. More critically, even when signatures are present, they can be removed or detached in workflows that preserve the appearance of legitimacy while altering the underlying artifact.

Capability	PKI	VeraFile
Protects filename	✗	☑
Full file coverage	✗	☑
Detects renaming	✗	☑
Works without infrastructure	✗	☑

In practice, the adversary's attack surface is not the cryptographic system - it is the file that no longer carries its protection.

Reframing Integrity: *From Systems to Artifacts*

The fundamental issue is not the absence of integrity controls, but their placement. Current architectures attempt to enforce integrity through systems, infrastructure, and processes - controls inherently bound to their specific environments. Files, by contrast, are mobile. They cross boundaries that systems cannot.

To close the integrity gap, trust must be bound directly to the artifact itself. The file must become capable of proving its own integrity, independent of the systems that create,

transmit, store, or process it. This shift from system-centric trust to artifact-centric trust is not an incremental improvement; it is architectural reorientation.

VeraFile: *Establishing Portable File Identity (The Cryptographic Mechanics)*

VeraFile implements this shift through the introduction of Verification Integrity Keys *(VIKs)* – compact, human readable, cryptographic identifiers derived from a file's content, name, and structural attributes. The VIK is embedded directly into the filename, creating a persistent, visible, and verifiable trust anchor between the file and its identity.

Built on SHA-512 cryptographic internals, the system uniquely binds the filename to the file contents without requiring complex management or exchange of traditional cryptographic keys. Instead, the VIK functions as a composite identifier containing the validation state, VIK length, policy routine, and the core integrity key value.

Validation is elegant and stateless: the system simply recalculates the VIK based on the base filename, metadata, and contents, and confirms a match with the VIK embedded in the filename. For example, a sealed operational artifact appears as:

Target_data3.V8a-4b2KT9mP

(Note: The PDF of this whitepaper has been both signed and sealed, serving as a real-world example of a VIK sealed PKI signed document.)

This produces a simple but powerful outcome: the file becomes self-validating. Integrity can be assessed at any point in the file's lifecycle without reliance on external systems, keys, or infrastructure. The file does not need to be opened, parsed, or modified. It carries the information necessary to verify itself wherever it exists, transforming integrity from an environmental property into an intrinsic property of the file.

Integrity That Survives Real-World NSS Conditions

National Security Systems operate in conditions inherently hostile to traditional integrity mechanisms. VeraFile is designed specifically for these environments:

- **Unbreakable Continuity:** Because the integrity marker is embedded in the filename, it survives movement through email systems, cloud platforms, removable media, and cross-domain solutions. It is not dependent on fragile metadata or access controls.
- **Content Agnosticism:** VeraFile operates without requiring access to the file's internal content. This enables validation for encrypted or access-restricted files without violating handling policies or exposing sensitive data.

- **Universal Application:** VeraFile can seal any file type - newly created or decades old – encrypted and/or PKI signed.
- **Human Readability:** VeraFile's VIK delivers cryptographic integrity in a human-readable form, bridging the gap between security and human workflows by making trust visible to both systems and people.

The result is an integrity mechanism that aligns with the operational realities of NSS rather than the assumptions of controlled environments.

Operational Implications for National Defense

The introduction of artifact-level integrity has immediate, high-impact implications for connected and air-gapped defense operations:

1. **Post-Compromise Recovery:** When systems can no longer be trusted, VeraFile provides a means of independently verifying critical data outside the compromised environment, restoring trust when infrastructure is degraded.
2. **At-Scale Validation:** High-volume data streams *(logs, telemetry, baselines)* can be validated continuously without the overhead of traditional cryptographic signing.
3. **Cross-Domain & Coalition Operations:** VeraFile offers a neutral trust mechanism that does not depend on shared PKI roots or coordinated infrastructure, providing a consistent integrity signal regardless of the systems involved.

These capabilities address a set of challenges that existing models have not been able to solve at scale.

Flexible Deployment Architecture

VeraFile is lightweight software designed to integrate seamlessly into existing defense environments without heavy infrastructure overhead. It can be deployed in the following ways:

- **Endpoint & System Plug-ins:** As an integrated extension for browsers, native file systems, or endpoint protection platforms such as Microsoft Defender and CrowdStrike Falcon.
- **Background Service:** As a no-code, real-time sealing service optimized for high-volume environments - such as application log generation pipelines.
- **Native API:** As an API embedding automated sealing and validation capabilities directly inside custom applications or document or file production systems.
- **Automated Validation:** As a scheduled task to enforce continuous, zero-touch validation across resting enterprise data.

- **High Trust Implementation:** A split-processing architecture that isolates the VIK calculation from the local environment using out-of-band cryptographic secrets *(peppering)*. This ensures artifact integrity can be generated and validated even in deeply compromised local environments.

Complementing, Not Replacing, Existing Controls

VeraFile does not replace PKI or other cryptographic mechanisms; it addresses the critical gaps in integrity those mechanisms leave exposed.

PKI establishes identity and intent *(who signed a file and under what authority)*. VeraFile establishes immutability in context *(whether the file, including its name and structure, remains exactly as it was when created)*. In combination, these approaches can provide a more complete model of trust. Separately, each leaves gaps that adversaries can exploit.

Accelerating Compliance: *Mapping VeraFile to Federal Mandates*

Within National Security Systems, compliance is often treated as a retrospective exercise - an administrative function that validates controls after the fact through documentation, boundary enforcement, and periodic assessment. This approach creates inherent friction. It relies on system-centric evidence, assumes stable control boundaries, and depends heavily on point-in-time validation in environments where data is constantly moving beyond those boundaries.

VeraFile fundamentally alters this model by shifting integrity from a ***system-enforced condition*** to a ***data-intrinsic property***. By cryptographically binding the filename to the file's contents, without reliance on key infrastructure or persistent connectivity, VeraFile enables integrity to be continuously verifiable - anywhere.

In doing so, VeraFile does not introduce a new compliance framework. It ***accelerates and strengthens*** existing mandates by ensuring that the underlying data artifacts remain trustworthy across the full lifecycle envisioned by those mandates.

The DoD Zero Trust Strategy *(Data Pillar)*

The Department of Defense Zero Trust architecture mandates a shift away from perimeter-based defense toward *"data-centric security."* Zero Trust calls for a transition from perimeter-based defense to a model centered on protecting data itself. A core principle of the Data Pillar is that information must remain secure, attributable, and verifiable across all environments, including those that are untrusted or compromised.

> *VeraFile directly operationalizes this requirement.*

By establishing a Portable File Identity *(PFI)*, VeraFile removes the implicit dependency on network, endpoint, or enclave trust. Each file becomes independently verifiable, enabling integrity validation even in scenarios where systems are degraded, breached, or outside the control boundary. This aligns precisely with the Zero Trust assumption of breach - not at the system level, but at the artifact level where decisions are made.

Rather than relying on infrastructure to assert trust, VeraFile allows data to be cryptographically verified, independently of any system, network, or infrastructure.

NIST SP 800-53 - *System and Information Integrity (SI) and Audit (AU)*

Federal systems operating under NIST SP 800-53 are required to implement controls that ensure the integrity of information and detect unauthorized modification. Controls such as SI-7 *(Software, Firmware, and Information Integrity)* and AU-2/AU-9 *(Audit Events and Protection of Audit Information)* are foundational to this requirement.

In practice, these controls are typically implemented through file integrity monitoring (FIM), logging systems, and audit trails that are tightly coupled to specific infrastructure. While effective within controlled environments, these mechanisms lose visibility and enforcement capability once data is exported, transferred, or processed externally.

VeraFile extends the intent of these controls beyond their traditional boundaries.

By embedding a persistent integrity anchor directly into the file, it enables continuous, stateless validation without reliance on the originating system. Files can be validated anywhere, at any time, without requiring access to logs or centralized monitoring systems. This not only strengthens SI-7 compliance but also reduces the operational burden associated with demonstrating it, particularly in distributed or cross-domain architectures.

The result is a shift from ***environment-dependent integrity assurance*** to ***artifact-level integrity assurance***, which closely aligns with the realities of modern NSS data flows.

NIST SP 800-171 and CMMC - *Protecting CUI Across the Supply Chain*

Defense Industrial Base *(DIB)* contractors must protect Controlled Unclassified Information *(CUI)* under DFARS 252.204-7012, which mandates compliance with NIST SP 800-171 and the Cybersecurity Maturity Model Certification *(CMMC)*. A persistent challenge in these environments is maintaining the integrity of CUI as it moves between organizations, systems, and classification levels.

VeraFile addresses this challenge by maintaining a continuous cryptographic linkage between the file's identity and its content. With VeraFile, as CUI traverses the supply chain, between prime contractors, subcontractors, and government systems, its integrity remains independently verifiable. Even in cases of misrouting, spillage, or handling within

unmanaged environments, the file retains its original identity and can be validated without reliance on the originating infrastructure.

For Authorizing Officials and assessors, this provides a mitigating control, a form of mathematical assurance that the artifact has not been altered, reducing ambiguity in compliance determinations and strengthening trust across organizational boundaries.

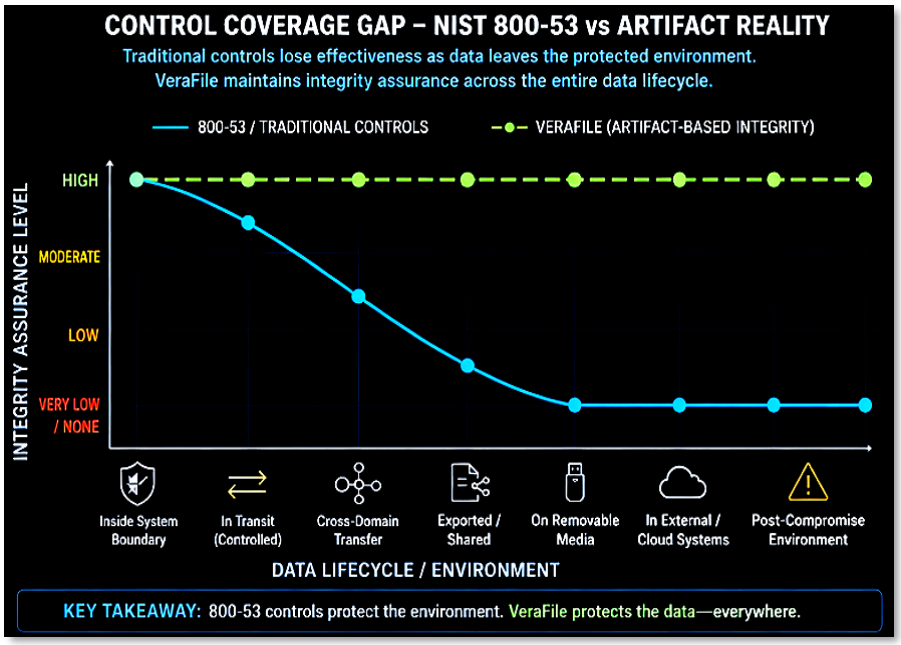
Reducing the Audit Burden Through Artifact-Level Proof

One of the most persistent challenges in federal compliance is the fragmentation of evidence required to demonstrate control effectiveness. Organizations must correlate logs, endpoint telemetry, access records, and cryptographic artifacts to establish that a given file is authentic and unaltered.

For files and documents, VeraFile collapses this complexity.

By embedding verifiable integrity directly into the file, it eliminates the need to reconstruct trust through multiple external systems and complex chains of custody. Validation becomes immediate and deterministic. The file does not require supporting evidence - it is the evidence.

This has direct implications for RMF and ATO processes. Instead of relying solely on inherited controls and environmental assurances, organizations can demonstrate that integrity persists with the data itself, even when those controls are no longer present.



Strategic Implication

VeraFile does not replace existing compliance frameworks. It enables them to function as intended in environments where traditional assumptions about control boundaries no longer hold.

- Compliance is no longer something that must be proven after the fact. It becomes a property that is continuously carried by the data itself.

Conclusion

National Security Systems are no longer targeted solely for unauthorized access. Increasingly, adversaries focus on data manipulation - subtly altering logs, reports, configurations, and intelligence in ways that evade detection yet directly influence decisions. These attacks are high-impact, low-visibility, and are unfortunately well-aligned to modern operational workflows.

Current architectures are not designed to stop them. They enforce integrity through systems, networks, and controls that do not persist with the data they are intended to protect. Once a file leaves those boundaries, or is manipulated within them without triggering system-level alerts, trust becomes assumed rather than proven. VeraFile addresses this gap by anchoring integrity where it ultimately matters: ***the artifact itself***.

By cryptographically binding identity to both the file's contents and its name, VeraFile ensures that integrity is not inherited from a system, but carried with the data - portable, persistent, and independently verifiable across trusted and untrusted environments and domains - including compromise.

This represents a shift in security architecture: from system-centric trust to artifact-centric trust.

- *The question is no longer whether systems can be trusted. It is whether the data they produce, store, and move can prove itself.*

The future of national defense data integrity no longer relies on the infrastructure that carries it. With VeraFile, integrity is inextricably bound to the file.

Control Coverage vs. Data Lifecycle

Data State	800-53 Control Coverage	Actual Integrity Assurance	VeraFile Coverage
Inside system boundary	**High**	**High**	**High**
In transit *(controlled)*	**High**	Moderate	**High**
Cross-domain transfer	Moderate	**Low**	**High**
Exported / shared	**Low**	**Very Low**	**High**
On removable media	**Low**	**Very Low**	**High**
In external/cloud systems	Moderate	**Low**	**High**
Post-compromise environment	**None**	**None**	**High**

Addendum - *NIST 800-53 Crosswalk & ATO Evidence*

Control	Control Intent	Traditional Implementation Limitation	VeraFile Contribution
SI-7 Software, Firmware, and Information Integrity	Detect unauthorized changes to data	Relies on FIM tied to specific systems; no visibility once files move	Enables **continuous, location-independent validation** of file integrity
SI-4 System Monitoring	Monitor system activity for anomalies	Dependent on system telemetry; cannot detect offline or post-transfer tampering	Provides **deterministic integrity validation** independent of system monitoring
AU-2 Audit Events	Record events necessary for monitoring	Captures actions, not the **state of the file after movement**	Allows validation of **actual artifact state**, reducing reliance on reconstructing events
AU-9 Protection of Audit Information	Protect audit logs from tampering	Logs are vulnerable once exported or aggregated externally	Ensures logs remain **tamper-evident wherever stored or analyzed**
SC-16 Transmission of Security Attributes	Protect attributes associated with data	Attributes often lost or altered across systems	**Binds identity to file itself**, eliminating reliance on external attributes
CM-5 Access Restrictions for Change	Limit unauthorized modifications	Enforcement ends at system boundary	Detects **unauthorized change regardless of where it occurs**

Dimension	Traditional ATO Evidence Model	With VeraFile
Evidence location	Distributed across systems	Embedded in file
Validation method	Correlation and inference	Direct verification
Lifecycle coverage	Limited to system boundary	Persistent across lifecycle
Cross-domain assurance	Weak	Strong
Audit complexity	High	Low
Confidence level	Conditional	Deterministic

Addendum – *Perception vs. the Integrity Gap*