THE UNSEEN VULNERABILITY IN FEDERAL NETWORKS

Closing the File Integrity Gap to Meet Zero Trust Mandates

Abstract v1.1

If you can't prove the integrity of your data, you don't have Zero Trust - you have blind trust.

VeraSec Technologies

Brian Hajost
bhajost@verasec.net

About VeraSec Technologies

VeraSec Technologies is a pioneer in digital artifact integrity, 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 technologies empower files to carry their own verifiable identity - preparing them for an actual Zero Trust world.

Operating at the forefront of Portable File Identity (PFI), 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, VeraSec helps organizations establish durable, portable trust in every digital asset, signed or un-signed - wherever it travels.

About The Author

Brian Hajost 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.

A Note on the Data

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, DoD, and DIB environments will exhibit variance based on specific mission architecture and internal IT policies.

The Unseen Vulnerability in Federal Networks: *Closing the File Integrity Gap to Meet Zero Trust Mandates*

Executive Summary

As the Department of Defense (DoD) and federal agencies aggressively pursue the mandate to achieve targeted Zero Trust goals by 2027, significant investments have been made in identity, credential, and access management (ICAM), as well as data-at-rest encryption. Yet, a fundamental vulnerability remains largely unaddressed: the lack of verifiable data integrity for the vast majority of stored information. Unstructured data—spanning system audit logs, Controlled Unclassified Information (CUI), automation scripts, and application telemetry, comprises roughly 80% to 90% of all agency and defense contractor data.

An analysis of typical network environments reveals a stark reality: over 95% of files exist without cryptographic proof of origin or structural integrity. While Public Key Infrastructure (PKI), exemplified by the ubiquitous CAC/PIV smart card system - remains the gold standard for human identity and securing high-value assets, it fundamentally fails to scale across the sheer volume, velocity, and variety of autonomous machine data and everyday unstructured files.

This white paper examines the structural limits of traditional PKI within federal networks, the necessity of defense-in-depth strategies to protect existing PKI investments, and the critical role of modern, keyless integrity solutions in satisfying stringent NIST and DFARS requirements. By decoupling integrity validation from the burdensome lifecycle of cryptographic key management, agencies and the Defense Industrial Base (DIB) can finally secure the remaining 95% of their unstructured data, ensuring true operational resilience and compliance.

The Federal Data Landscape: *A Crisis of Volume*

Understanding the file integrity gap requires categorizing how data is generated, stored, and secured across government and defense networks. The following breakdown illustrates the estimated distribution of file categories and the rate at which discrete PKI signatures are applied within each.

1. Audit Logs & Machine Data (35% – 45% of total files)

   PKI Adoption: < 1%

   The Challenge: Continuous monitoring telemetry, SIEM ingestion data, and security events represent the largest data segment. The velocity of log generation makes discrete PKI signing computationally prohibitive.

   The Compliance Risk: NIST SP 800-171 (3.3.8) and NIST SP 800-53 (AU-9) mandate the protection of audit information from unauthorized modification. If a nation-state actor alters logs to cover their lateral movement, cyber commands cannot mathematically prove the integrity of their telemetry.

2. Office Files & CUI (20% – 30% of total files)

   PKI Adoption: < 2%

   The Challenge: The bulk of daily unstructured data consists of internal memos, operational planning drafts, and CUI. While CACs are used to encrypt emails or sign high-level approvals, the friction of applying discrete certificates to every draft file created by personnel is operationally unfeasible.

   The Compliance Risk: Failure to protect the integrity of CUI constitutes a direct violation of DFARS 252.204-7012, risking loss of contract eligibility and Authority to Operate (ATO).

3. Backups & Archives (15% – 20% of total files)

   PKI Adoption: < 1%

   The Challenge: Cold-storage archives and disaster recovery backups are frequently encrypted for confidentiality, but rarely secured with discrete, file-level PKI certificates for continuous integrity validation.

   The Compliance Risk: Advanced Persistent Threats (APTs) increasingly target backup repositories. If backups are subtly corrupted, agencies may unknowingly restore compromised data, crippling mission readiness.

4. PDFs & Formal Documentation (10% – 15% of total files)

   PKI Adoption: 5% – 10%

   The Challenge: Driven by formal e-signature requirements for federal acquisitions, DD forms, and compliance, PDFs see the highest rate of business-process signing.

However, the vast majority of PDFs (manuals, scanned intelligence reports) remain unsigned.

5. Software & DevSecOps Scripts (5% – 10% of total files)
   PKI Adoption: 40% – 60%

   The Challenge: Commercial binaries are highly regulated. However, within agile DevSecOps pipelines, internal automation scripts (Bash, PowerShell) and rapid-deployment containers are frequently left unsigned to avoid slowing down deployment timelines.

   The Compliance Risk: Unsigned automation scripts bypass NIST SP 800-53 (SI-7) software integrity controls, allowing an attacker to distribute malware natively through a trusted federal CI/CD pipeline.

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%

The PKI Bottleneck: *Why Traditional Trust Fails at Scale*

The U.S. government's implementation of PKI is arguably the largest and most successful in the world. However, it is constrained by its own architecture when applied to high-volume, unstructured machine data.

Lifecycle Overhead: Issuing, rotating, and revoking cryptographic keys for millions of daily system files creates an untenable management overhead for federal IT departments.

Infrastructure Costs: Extending true PKI requires localized Hardware Security Modules (HSMs) and continuous auditing, which is difficult to deploy at the tactical edge or aboard forward-deployed assets.

DevSecOps Friction: For high-velocity software factories, the friction introduced by pausing to request, retrieve, and apply a cryptographic key often outweighs the perceived security benefits, leading developers to bypass signing protocols.

Defense in Depth: *Securing the PKI Foundation*

While extending PKI to ubiquitous unstructured data is administratively unfeasible, critical vulnerabilities persist even within the 5% to 10% of files that are successfully signed. A digital signature authenticates the origin and integrity of a payload at the exact moment of signing, but it does not inherently protect the file object itself from subsequent environmental manipulation by sophisticated adversaries.

Nation-state actors frequently target the "soft underbelly" of PKI-secured federal environments using techniques designed to bypass signature validation entirely.

Signature Stripping: If an attacker carefully strips the signature block from a critical binary, the OS may treat it as a standard, unsigned internal file, allowing it to execute and bypass strict validation checks.

Downgrade and Rollback Attacks (File Replacement): An adversary may replace a newly patched, securely signed executable with an older, vulnerable version of that exact same file. Because the older file still bears a mathematically valid PKI signature from a trusted DoD/Federal CA, traditional security controls will allow it to execute.

Certificate Compromise: If an agency's private keys are compromised, attackers can mint valid signatures for malicious payloads, blinding the entire PKI trust model.

The Keyless Overlay: *A Decoupled Safety Net*

To protect high-value, PKI-signed assets from these evasion tactics, agencies can overlay keyless integrity solutions as a secondary layer of defense. Technologies like VeraSec's VeraFile act as an independent protector for the PKI infrastructure itself.

Because this architecture completely circumvents the PKI bottleneck, operating flawlessly without using or managing cryptographic keys - it establishes a decoupled trust anchor. This provides three critical security advantages for already-signed files:

Tamper-Evident Signatures: A keyless integrity monitor continuously validates the state of the entire file object. If an attacker attempts signature stripping, the overall mathematical state of the file changes, triggering an undeniable alert to the SOC.

Stateful Anti-Rollback Protection: Keyless ledgers establish chronological proof of a file's state. If a threat actor attempts a rollback attack using a legitimately signed but vulnerable older version, the keyless solution immediately flags the state regression.

Resilience Against CA Compromise: Because the keyless overlay is technologically isolated, an attacker who compromises an agency's private keys cannot alter the keyless integrity proofs. The independent ledger instantly highlights discrepancies.

The Cost of Inaction: *Mission Degradation and Compliance Failure*

The assumption that network firewalls and ICAM negate the need for file-level integrity is a dangerous remnant of perimeter-based security.

When data integrity is compromised silently by an APT dwelling in a network, the DoD and DIB face:

Loss of Authority to Operate (ATO): Inability to verify the integrity of critical systems leads to immediate decertification under the Risk Management Framework (RMF).

Failed CMMC Audits: DIB contractors who cannot demonstrate continuous file integrity monitoring risk failing Cybersecurity Maturity Model Certification assessments, jeopardizing future contract awards.

Compromised Mission Readiness: If commanders cannot mathematically verify that operational plans, target coordinates, or logistics databases are in their original, unmanipulated state, the mission cannot proceed safely.

Bridging the Gap: *The Shift to Keyless Integrity Validation*

To meet the Data Pillar objectives of the DoD Zero Trust Strategy and align with controls in NIST SP 800-53 and NIST SP 800-171, agencies must move beyond traditional File Integrity Monitoring (FIM) toward continuous, file-native cryptographic validation.

Conventional approaches based on Public Key Infrastructure (PKI) do not scale across the full data landscape. Key management overhead, signing latency, and format limitations leave most enterprise data, especially logs, scripts, and operational artifacts, without persistent cryptographic identity.

Technologies such as VeraSec's VeraFile introduce a keyless integrity model, embedding a portable cryptographic identity (Validation Integrity Key, or VIK) directly into each file. Derived from the file's content, name, and size, this identity enables independent validation without certificates, keys, or supporting infrastructure.

This approach allows organizations to:

- Validate files continuously at scale
- Maintain integrity across systems and environments
- Extend protection to high-volume, transient data

By eliminating reliance on key management while preserving cryptographic assurance, keyless validation enables agencies to prove data integrity continuously, closing a critical gap in Zero Trust architectures - particularly for data types that PKI cannot practically protect.

Conclusion: *Securing the Foundation of Federal Zero Trust*

The file integrity gap represents one of the most critical attack surfaces in the modern federal enterprise. Relying solely on perimeter defenses, access controls, and data-at-rest encryption leaves government systems dangerously exposed to adversaries designed to subvert networks from the inside out.

Traditional PKI, burdened by the heavy administrative friction of certificate lifecycles, simply cannot scale to protect the velocity and volume of agency data. By adopting modern, keyless integrity validation methods, organizations can secure the vulnerable 95% of their unstructured data while providing a frictionless, independent overlay that hardens the existing 5% of PKI-signed assets against advanced evasion tactics.

The DoD Zero Trust Strategy mandates that trust is never assumed, yet federal networks routinely assume the structural integrity of millions of internal files every day. Continuously proving the mathematical integrity of every file is no longer an optional security enhancement; it is a fundamental requirement for national security, regulatory compliance, and operational dominance.

If you can't prove the integrity of your data, you don't have Zero Trust - you have blind trust.

Addendum A

NIST SP 800-53 Rev. 5 Control Mapping for Keyless Integrity

Achieving an Authority to Operate (ATO) and maintaining compliance under the Risk Management Framework (RMF) requires strict adherence to NIST SP 800-53. Traditional File Integrity Monitoring (FIM) and PKI solutions often struggle to meet these controls at the scale of modern federal data without introducing massive administrative overhead.

Because VeraSec's VeraFile establishes irrefutable proof of file state and entirely circumvents the PKI bottleneck, operating natively without using or managing cryptographic keys - it uniquely satisfies critical NIST controls across high-volume, unstructured datasets.

Below is a cross-reference of key NIST SP 800-53 controls and how a keyless integrity overlay satisfies them:

System and Information Integrity (SI Family)

- **SI-7: Software, Firmware, and Information Integrity**
  - *Control Requirement:* Employ integrity verification tools to detect unauthorized changes to software, firmware, and information.
  - *VeraFile Capability:* Provides continuous, tamper-evident validation for unstructured data, DevSecOps scripts, and CUI. It establishes chronological, stateful proof that instantly flag signature stripping, file manipulation, or unauthorized modification without the overhead of issuing or rotating PKI certificates.

- **SI-7(6): Cryptographic Protection**
  - *Control Requirement:* Implement cryptographic mechanisms to detect unauthorized changes to software and information.
  - *VeraFile Capability:* Utilizes advanced hashing and scalable ledger mechanics to provide cryptographic certainty of file state. By eliminating the need to secure, rotate, or revoke keys, it provides the required cryptographic protection without the fragility of traditional key management infrastructure.

Audit and Accountability (AU Family)

- **AU-9: Protection of Audit Information**
  - *Control Requirement:* Protect audit information and audit tools from unauthorized access, modification, and deletion.

- *VeraFile Capability:* Machine-generated audit logs are created at a velocity that breaks traditional PKI signing. VeraFile continuously monitors log files, providing immutable proof that telemetry data has not been altered or deleted by a threat actor attempting to cover their tracks prior to SIEM ingestion.

Configuration Management (CM Family)

- **CM-5: Access Restrictions for Change**
  - *Control Requirement:* Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
  - *VeraFile Capability:* Acts as an independent, decoupled auditor. Even if an adversary bypasses logical access controls (e.g., via compromised credentials) to alter a configuration file or downgrade a signed binary (a rollback attack), VeraFile immediately flags the mathematical state regression.

Contingency Planning (CP Family)

- **CP-9: Information System Backup**
  - *Control Requirement:* Conduct backups of user-level information, system-level information, and security-related documentation. Protect the confidentiality, integrity, and availability of backup information.
  - *VeraFile Capability:* Ransomware variants increasingly target and subtly corrupt federal backup repositories. VeraFile continuously validates the structural integrity of cold storage and backup archives, ensuring that recovery teams do not unknowingly restore compromised or manipulated data during a contingency event.

Supply Chain Risk Management (SR Family)

- **SR-4: Provenance**
  - *Control Requirement:* Maintain the provenance of systems, system components, or software.
  - *VeraFile Capability:* By establishing chronological, immutable proofs of file states from the moment of creation throughout the data lifecycle, the keyless overlay provides a continuous chain of custody and provenance for critical software deployments and unstructured CUI.

Addendum B

CMMC 2.0 Maturity Level Mapping for Keyless Integrity

For Defense Industrial Base (DIB) contractors, achieving Cybersecurity Maturity Model Certification (CMMC) 2.0 is a prerequisite for contract eligibility. CMMC intimately ties to NIST SP 800-171, but categorizes controls into strict maturity levels based on the type of information handled - Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).

Traditional File Integrity Monitoring (FIM) and PKI architectures often create difficult compliance hurdles for small-to-medium DIB contractors due to the sheer cost and administrative burden of managing cryptographic keys. VeraSec's VeraFile accelerates CMMC readiness across multiple maturity levels by providing mathematically irrefutable integrity validation natively, completely circumventing the need to use or manage keys.

Below is a breakdown of how a keyless integrity overlay supports specific CMMC 2.0 maturity levels.

Level 1: *Foundational (Safeguarding FCI)*

Level 1 focuses on basic cyber hygiene and the protection of Federal Contract Information.

- **Relevant Domain:** System and Information Integrity (SI)
- **How Keyless Integrity Applies:** While Level 1 relies primarily on basic perimeter and endpoint defenses (antivirus), a keyless integrity overlay provides an automated safety net. It continuously monitors foundational system files and baseline configurations, providing immediate, tamper-evident alerts if malicious code bypasses traditional endpoint defenses and attempts to alter operational files.

Level 2: *Advanced (Protecting CUI - Aligned with NIST SP 800-171)*

Level 2 is the critical threshold for contractors handling CUI and requires full compliance with the 110 controls of NIST SP 800-171.

- **Audit and Accountability (AU.L2-3.3.8 - Protect Audit Information):** *CMMC Requirement:*
  - Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
  - *VeraFile Application:* Because it handles high-velocity data without the friction of key issuance, VeraFile continuously validates the state of machine-generated audit logs. It provides DIB contractors with mathematically undeniable proof during a CMMC assessment that their telemetry data has not been tampered with.

- **System and Information Integrity (SI.L2-3.14.3 - Unrecognized System Alerts):** *CMMC Requirement:*
  - Monitor system security alerts and advisories and take action in response.
  - *VeraFile Application:* Silent data manipulation - where an adversary alters a CUI document or deployment script without triggering malware signatures, often goes unrecognized. The keyless ledger instantly flags these mathematical state changes, turning invisible tampering into an immediate, actionable security alert.

Level 3: *Expert (Defending Against APTs - Aligned with NIST SP 800-172)*

Level 3 is reserved for the most critical DIB contractors facing Advanced Persistent Threats (APTs) and requires proactive, defense-in-depth architecture.

- **System and Information Integrity (SI.L3-3.14.3e - Verify Integrity of Critical Software):**
  - *CMMC Requirement:* Verify the integrity of critical software and information using cryptographic mechanisms.
  - *VeraFile Application:* APTs actively target PKI infrastructure to mint forged signatures or execute rollback attacks using compromised certificates. VeraFile acts as a decoupled, independent auditor for existing PKI. By proving the state of the file without relying on the network's underlying certificate authority, it stops signature stripping and downgrade attacks dead in their tracks, satisfying the highest tier of cryptographic integrity verification.