



Breaking New Ground in Government Identity Security

Thank you for downloading this 1Kosmos Whitepaper. Carahsoft is the master government aggregator and distributor for 1Kosmos Cybersecurity solutions.

To learn how to take the next step toward acquiring 1Kosmos' solutions, please check out the following resources and information:



For additional resources:
carah.io/1KosmosResources



For upcoming events:
carah.io/1KosmosEvents



For additional Thales TCT News:
carah.io/1KosmosProducts



For additional Cybersecurity solutions:
carah.io/CyberSecuritySolutions

To set up a meeting:
1kosmos@carahsoft.com



[703-889-9804](tel:703-889-9804)

For more information, contact Carahsoft or our reseller partners:
1kosmos@carahsoft.com | 703-889-9804

Breaking New Ground in Government Identity Security

Setting a New Standard for Identity Verification
and Full-Service Credential Service Providers



Executive Summary

Government agencies are under constant threat of cyber attack, yet most identity solutions force them into rigid systems that don't fit their actual needs. 1Kosmos takes a different approach—offering a flexible platform that adapts to how agencies actually work, from simple document verification to advanced digital identity wallets.

Our uniqueness flows beyond our platform's workflows – 1Kosmos has achieved something no other company has: both FedRAMP (Federal Risk and Authorization Management Program) High Authorization and Kantara certification. This dual certification means government agencies can obtain the highest security standards for Federal civilian agencies while maintaining the flexibility to deploy solutions that fit their specific requirements—whether they're protecting law enforcement data, financial systems, or health information.

The result is a platform that lets agencies start small and scale up as needed, all while giving citizens complete control over their personal information and maintaining the most stringent security available in the civilian market.

This whitepaper details the significance of this achievement, the rigorous requirements of FedRAMP High, and the unique value 1Kosmos brings to the public sector.

The FedRAMP High Standard: What It Means

Unmatched Security Foundation

1Kosmos is the sole CSP to simultaneously hold both FedRAMP High authorization and Kantara certification, positioning the platform at the forefront of government identity security solutions. Together, these certifications ensure that 1Kosmos meets both the practical needs of government operations and the technical standards required for secure digital identity systems.



Kantara Certification

Based on National Institute of Standards and Technology (NIST) 800-63-3 digital identity guidelines, validates that the platform operates according to the gold standard for identity verification processes and procedures.

FedRAMP High Authorization

Takes security to the next level, implementing over 400 security controls based on NIST 800-53 standards. This represents the most stringent civilian agency security requirements available, with only 20 additional controls separating High from IL4 defense-level certification.

Understanding FedRAMP Impact Levels

FedRAMP defines three security impact levels—Low, Moderate, and High—based on the sensitivity of data and the potential impact of a security breach. FedRAMP High is reserved for systems where a breach could have severe or catastrophic effects, such as mission failure or irreparable institutional damage. It requires 421 security controls, including advanced cryptography, automated flaw remediation, personnel screening, and boundary protection.

Impact Level	Controls	Typical Data	Impact if Compromised
Low	125	Public, non-sensitive	Limited adverse effects
Moderate	325	Sensitive but unclassified, PII	Serious adverse effects
High	421	Law enforcement, health, financial, mission-critical	Severe/catastrophic effects



Security and Privacy by Design

Comprehensive Protection Approach

1Kosmos takes a holistic approach to security that goes well beyond minimum compliance requirements. The platform's architecture incorporates privacy and security considerations at every level, reflecting the understanding that personal identity information is one of the most valuable and vulnerable data types in any system.

Multi-Layer Encryption Standards

All data within the 1Kosmos platform is protected using Federal Information Processing Standards (FIPS) 140-3 encryption, whether it's being transmitted between systems or stored in databases. The platform uses a two-stage encryption process for digital identity wallets: personal information is first encrypted using standard protocols, then encrypted again within each user's individual wallet. Importantly, users maintain exclusive control over their wallet encryption keys, meaning neither 1Kosmos nor government agencies can access personal data without explicit user permission.

Key Security Features:

Privacy by Design

End users have sole control over their information, protected by cryptographically paired public-private key architecture

Phishing-Resistant Authentication

Advanced multi-factor authentication credentials, including FIDO passkeys, device biometrics, and LiveID

Immutable Audit Trail

Every event is logged immutably, providing complete visibility into all logins and access attempts

Fraud Prevention

Passive liveness detection, injection monitoring, and triangulation of captured data against sources of truth

User Sovereignty

Neither 1Kosmos nor their customers can access end user wallet data without explicit user consent



FedRAMP High Authorization: The Assessment Journey

Achieving FedRAMP High required a rigorous, multi-month assessment process that demonstrates verified, not just claimed, security hardening through third-party assessment:

- Operating within a U.S. GovCloud environment, with U.S. citizens managing the environment and passing strict background checks
- Meeting FIPS 140-3 encryption standards for all data in transit and at rest
- Continuous monitoring and rapid remediation of vulnerabilities, with strict timelines based on criticality
- Adhering to over 400 NIST 800-53 controls, surpassing the requirements of ISO 27001 and SOC 2 certifications

1Kosmos leveraged the FedHive platform, a FedRAMP High authorized platform, to accelerate the process while maintaining the highest compliance standards.

Value for Government and Critical Infrastructure

End-to-End Capabilities

This dual certification approach provides Government buyers with unprecedented assurance. Whether at the Federal, State or Local levels, this certification combination simplifies vendor selection and reduces compliance risks. The FedRAMP High baseline ensures smooth flow-down compliance, eliminating the complexity of multiple security assessments.

With FedRAMP High Authorization and Kantara certification, federal agencies and contractors can use 1Kosmos to:

- Secure high-impact systems without compromising user experience or compliance
- Modernize digital identity systems and protect against advanced threats like identity impersonation, credential compromise, and account takeover
- Ensure adherence to NIST, FIPS, and Executive Order/OMB mandates
- Deploy a privacy-first, user-controlled digital identity wallet, reducing the risk of data breaches and regulatory non-compliance
- Scale from simple document capture to comprehensive identity lifecycle management



Proven Global Scale and Performance

The platform's global deployment success stories demonstrate scalability and reliability under real-world conditions. One global business process outsourcing company successfully transitioned half their worldwide user base to 1Kosmos authentication within just two months, showcasing the platform's ability to handle massive-scale implementations without compromising security or performance.

Similarly, 1Kosmos is deployed across multiple retail environments in North America to perform secure, in-person identity verification. In one case, after rolling out the solution to just one-third of its locations, a major retailer saw fraud losses drop by over 50%—demonstrating the immediate impact of identity assurance at the point of service.

Operational Flexibility

1Kosmos's modular architecture allows agencies to deploy solutions ranging from simple document capture to comprehensive digital identity wallets, scaling as requirements evolve. The platform's privacy-first data retention philosophy ensures that only necessary data is stored, using user-controlled encryption keys.



Conclusion

1Kosmos's dual certification as both a FedRAMP High authorized and Kantara-certified CSP sets a new standard for digital identity security in the public sector. This unique combination provides government agencies with unmatched assurance, flexibility, and privacy protection while enabling them to scale from basic identity verification to comprehensive digital wallet solutions.

As agencies accelerate digital transformation initiatives, the 1Kosmos platform delivers the security foundation necessary to confidently expand digital services while maintaining the highest protection standards for citizen data. With plans to extend certification to IL4 levels for defense customers, 1Kosmos continues advancing government identity security capabilities.

The FedRAMP High authorization empowers organizations to modernize identity systems, combat advanced threats, and protect sensitive data with confidence—establishing

1Kosmos as the definitive choice for comprehensive government identity security solutions.

1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers, and residents to securely engage with digital services. The company performs millions of authentications daily for major banks, telecommunications providers, technology and service providers, healthcare organizations, and retailers worldwide.