NUTS Technologies®

MISSION STATEMENT

To provide built-in data-centric cybersecurity that protects mission systems and enables the warfighter to execute operations with trusted data and high assurance in contested environments.

CAPABILITY STATEMENT

CAPABILITIES

Delivering Modular High Assurance Control by applying modular cryptography at the data layer, rather than relying on monolithic platforms, perimeter defenses, or infrastructure-bound security controls.

Enabled by two foundational technologies:

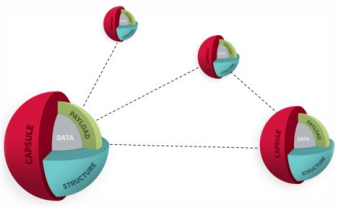
- **SDFT (Structured Data Folding with Transmutations) -** a cipher-neutral, crypto-agile data transformation protocol validated through NIST SBIR Phase I research for easing the transition to post-quantum cryptography.
- **Nut Capsules** - cryptographically self-governing data objects created using SDFT that embed encryption, fine-grained access control, policy, provenance, and governance directly into the data.

PAST PERFORMANCE

- **NIST SBIR Phase I -** Easing the transitions to post-quantum cryptography (Helps to satisfy NSA CNSA 2.0 requirements).
- **NAVY SBIR Phase I** - Self-hosted autonomous Certificate Key Management System.
- **DAF SBIR Phase I Open Topic** - Insider Threat Defense, mitigating insider threats at the data object layer (Zero Trust/ Zero Trust Data Pillar).
- **DAF SBIR Phase I Open Topic** - SDFT (Structured Folding with Transmutations), message level crypto-agility to future proof DAF systems (Helps to satisfy NSA CNSA 2.0 requirements).

COMPANY DATA

CAGE: 808H8
UEI: N89NGZMW2CV3
DUNS: 080959339
Established: 2016
NAICS CODE:
541715,541511,
541512,561990



Address:
NUTS Technologies
336 Hazel Ave., Unit 517
Glencoe, IL. 60022

POC: Sotir Triantafillou, Co-Founder
sotir@nutstechnologies.com – (561)-617-6030
General Email: defense@nutstechnologies.com
https://www.nutstechnologies.com

CORE COMPETENCIES

Data-Centric Cybersecurity
Embedding security controls directly within data objects.

Cryptographic Policy Enforcement
Enforcing access and governance policies through cryptography rather than infrastructure.

Secure Cross-Domain Information Sharing
Trusted data exchange across classification levels and coalition networks.

Quantum-Resilient Cryptography
Crypto-agile architecture enabling migration to post-quantum cryptography.

Mission Data Governance
Binding policy, identity, and provenance directly to data.

Cyber-Resilient Data Infrastructure
Maintaining security and operational capability in degraded or contested environments.

DIFFERENTIATORS

- Built-In Data Security
- Cryptographic Enforcement of Data Owner Intent
- Data-Centric Zero Trust (Data Pillar)
- Fine-Grained Cryptographic Access Control
- Crypto-Agile and PQC Ready
- Policy, Identity, and Provenance Bound to Data
- Portable Across Any Environment
- Resilient in Contested Environments
- Data-Defined Networks

DoW CRITICAL TECHNOLOGY AREAS

Strong alignment

- Quantum & Battlefield Information Dominance
- Applied Artificial Intelligence (secure data for AI)

Operational alignment

- Cyber & Networks Directorate
- C3BM leadership
- Electronic Systems Directorate
- Platform One / DevSec Ops ecosystem
- NC3 program offices

Awardable on the Tradewinds CDAO Marketplace

Secure generative AI (GAINE)

Insider Threat Defense (ITD)