

Supporting Those Who Protect Our Freedom

ASSYST provides defense technology solutions, platforms, applications, systems, and commercial innovations that enable the Department of War (DoW) and the U.S. Army to achieve military objectives, sustain mission readiness, and protect national security interests. With over 30 years of mission experience, we deliver secure IT modernization, AI-driven compliance automation, and resilient infrastructure to strengthen our armed forces and safeguard critical assets.

- **Domains** - Enterprise IT Infrastructure & Cloud Services, Cybersecurity & Zero Trust Architecture, Command, Control, Communications, Computers, & Intelligence (C4I/C5ISR), Data Analytics, AI/ML, Decision Support, Application Development & Integration, Human Systems Integration & Training, Compliance, Risk, & Assurance, Disaster Recovery, Continuity of Operations (COOP) and Resilience, Cross-Domain & Multi-Domain Integration
- **Certifications** - CMMC L2 Self Assessed | CMMI Level 3 (SVC/DEV) | ISO 27001/20000/9001
- **Prime Contractor** - +40 Agencies, FedRAMP, NIST, FISMA, and Zero Trust aligned delivery
- **Contract Vehicles** - Army ITES-3S, MDA SHIELD IDIQ, CDAO AI Talent 2.0, GSA OASIS+, GSA MAS (Cloud, HACS, HEAL), NIH CIO-SP3
- **Partnerships** - ServiceNow, AWS, Microsoft, Databricks, Red Hat, Oracle
- **Solutions** - Green Accelerator powered Commercial Solutions Offerings



Serving DoW Commands, Components and Installations



Cyber Defense and Resilience

For Defense Human Resources Activity (DHRA), DLNSEO’s National Security Education Program (NSEP), ASSYST advances secure, resilient operations through Zero Trust, AI-driven vulnerability detection, and continuous monitoring. We modernized NSEP’s mission systems and cloud infrastructure to strengthen data protection, ensure uninterrupted access, and maintain compliance across sensitive DoW platforms.

Identity, Credential and Access Management

For multiple Defense Agencies and Installations, ASSYST delivers CAC/PIV-enabled identity services, RecAccess SaaS-based access platforms, and RBAC solutions that provide secure, role-based access across Defense computing environments. Our solutions modernize legacy access systems, enable interoperability, and protect sensitive personnel and mission data with enterprise authentication, authorization, and auditing.

Secure Software Modernization

Rapidly modernized US Department of Energy’s Facility and Personnel Access Management systems with low-code platforms, ICAM, and RBAC to replace critical aging infrastructure. The modernization established secure, role-based, and multi-agency access controls while integrating real-time monitoring and security visibility across national energy facilities. These improvements enhance operational resilience, reduce risk from outdated systems, and ensure that access to sensitive environments is managed with the highest standards of security and compliance.

C4ISR Integration

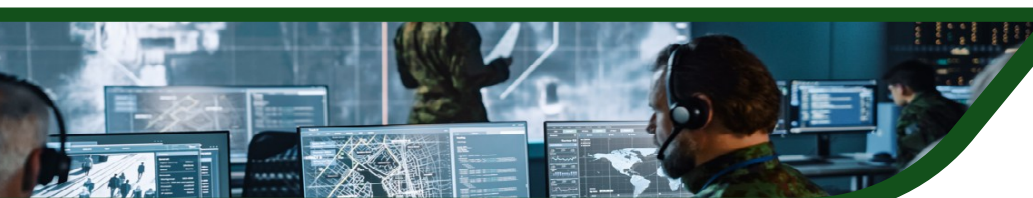
ASSYST supports the U.S. Army Installations with secure, enterprise communication and collaboration systems that enhance mission connectivity and coordination. We modernized legacy communication infrastructure into an integrated, cloud-enabled environment with advanced analytics and continuous monitoring. Our capability strengthens C4ISR operations, situational awareness, and real-time decision-making across defense networks.

Supply Chain Risk Management

Provide Subject Matter Expertise to ensure Defense Microelectronics Activity (DMEA) operations are performed efficiently with minimal disruption, especially during an emergency or crisis, by providing robust Continuity of Operations Planning (COOP), documentation, training, and exercises. For US Nuclear Regulatory Commission (NRC) ASSYST modernized and managed the core platform for tracking expenditures, cost recovery, and operational budgets. By moving to secure cloud infrastructure and embedding advanced analytics, the system now delivers real-time financial visibility, strengthens oversight and audit readiness, and aligns with NRC’s modernization and cybersecurity priorities—reinforcing regulatory transparency and supporting national energy security.

Data Analytics and AI

ASSYST is deploying AI/ML models that ingest diverse streams of security telemetry from US health and Human Services (HHS) CMS’s hybrid cloud and on-premises environments, detecting anomalies, correlating events, and enriching threat intelligence. These capabilities enable proactive identification of emerging risks and accelerate incident response. This integrated approach fuses signals from multiple domains to strengthen situational awareness and operational resilience. By applying these methods, CMS enhances protection of sensitive healthcare information, ensures compliance, and contributes to the broader mission of safeguarding critical national infrastructure.



**Defense Tech Services,
Partnering Opportunities, contact**

Loren Gray, Army Program Advisor
Eugene Goldlust, Sr. Account Executive
Joe Anderson, COO

