AIR FORCE NUCLEAR WEAPONS CENTER

Never Doubted, Always Feared

Rapid Testing at the Speed of War: *How an Experimental Other Transaction Authority (OTA) Unlocked IL5 Ephemeral Environments for Secure Tech Assessments*



Controlled by: AFNWC/NIY
CUI Category(ies): None
LDC/Distribution Statement: None
POC: afnwc.niy.workflow@us.af.mil

Introductions

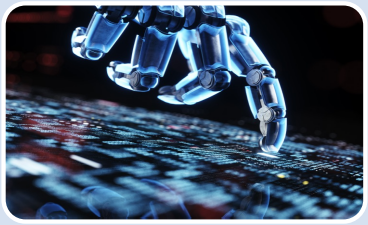
- Presenters:
  - ICBM Digital Futures Branch:
    - John Lundin, Program Manager, DAF
    - Dakota Wright, Program Manager, BAE
  - SHE BASH LLC:
    - Brandon Chanco – Information Systems Security Manager (ISSM)

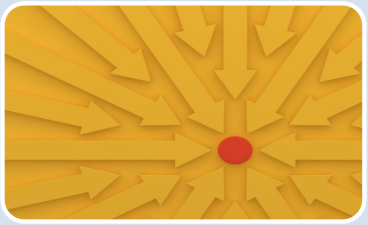
Agenda

- The Acquisition Half:
  - Who we are
  - The Catalyst
  - Phase 1- Incubation
  - Phase 2- Rapid Transition
  - Comprehensive Acquisition at Speed
  - Lessons Learned for Rapid Execution
- The Delivery Half:
  - Who is SHE BASH
  - The Platform: Dedzed
  - Ephemeral Environments, On Demand
  - Zero-Trust Access
  - The Automated Pipeline
  - Key Takeaways: The Dedzed Impact

Who we are: Digital Futures (NIYB)

NIYB: DIGITAL FUTURES BRANCH MISSION





Identify	Mature	Transition

Our Mission: Identify, mature, and transition Digital Capabilities that enhance the safety, security, and mission effectiveness of the ICBM weapon system

The Catalyst: The "PowerPoint" Problem

The Accelerator Loop: NIYB actively participated in "accelerator events" to discover cutting-edge small business technologies.

Pitch-Deck Bottleneck: At the end of these 8-week events, Digital Futures received highly impressive PowerPoint presentations and pitches outlining potential solutions.

No “Front Door” for Innovative Solutions: NIYB had an opportunity, create an environment to ingest, test, and evaluate the actual software to see if it performed as advertised.

"Try Before You Buy" Approach: An isolated sandbox (front door) to conduct hands-on, technology assessments for requirements validation before any final decisions are made.

Phase 1 Incubation (The SBIR Phase II)

The Birth of Dedzed: To solve our "front door" problem, we partnered with SHE BASH via a SBIR Phase II to prove the concept of a secure, on-demand assessment environment.

Key Validations During Incubation: We successfully demonstrated the feasibility of three core technical pillars:

Rapid, Ephemeral Cloud Provisioning	Integrated Security Tooling	Secure, Containerized Developer Access

The Transition Trigger: The SBIR was a success. It proved the core concepts were viable, creating the trigger to transition the concept into an accredited operational capability.

Phase 2 – Rapid Transition (The OTA)

The Challenge: Bridging the "Valley of Death"

- Transitioning a successful SBIR concept to a follow-on contract.
- Moving rapidly to prevent funding gaps.
- Maintaining the contractor's momentum and project continuity.

The Solution: A Strategic Transition via Experimental OTA

- Utilized a 10 U.S.C. § 4023 Experimental OTA to expedite the acquisition processes.
- Bypassed traditional FAR constraints to maintain rapid project momentum.
- Lowered the barrier to entry for our small business partner

Comprehensive Acquisition at Speed



The Accomplishment:

In just 3.5 months, executed the entire OTA award process, transitioning our SBIR partner to a follow-on contract without a funding gap.



Key Efforts Completed in 3.5 Months:

Drafted the Statement of Objectives (SOO).

Developed the Independent Government Cost Estimate (IGCE).

Finalized all Contract Data Requirements Lists (CDRLs).

Wrote the Determination & Findings (D&F) letter for Legal approval.

Conducted a full Technical Evaluation.



The Enablers of Our Speed:

Powered by the Human Element: This speed wasn't about the process; it was about the people—a trusted contractor partnership forged during the SBIR, and a knowledgeable Contracting Officer committed to our mission

Lessons Learned for Rapid Acquisition

The Core Lesson: Master Your Legal Authority

The Strategy: 10 U.S.C. § 4023 (Experimentation & Testing) over § 4022 for prototyping because it provided a more streamlined pathway for our software evaluation effort.

To gain Legal concurrence: Translated our modern DevSecOps work into the statute's legacy categories, directly from our D&F letter.

"Signal Supplies" = Defined as testing digital technology processing, digital signature verification, and software artifact integrity.

"Telecommunications" = Defined as testing secure data transmission, network security protocols, and secure collaboration capabilities.

The Supporting Lesson: Structure Your Team for Speed

- **Let Experts Propose the "How":** After an initial delay trying to write a prescriptive SOW we pivoted to a SOO, which let us define the "what" and empowered the vendor (the SMEs) to propose the "how."
- **Treat Acquisition as a Partnership:** Eliminate traditional information silos to move faster. Frequent, iterative syncing between the PMO, CO, and vendor ensures everyone stays aligned and empowers rapid decision-making.

The Delivery Imperative (The Handoff)



The Acquisition Reality: A rapid acquisition strategy is only half the solution. It must be paired with an equally rapid technical delivery platform.



The Next Phase: Transitioning to our industry partner SHE BASH LLC to explore the technical DevSecOps architecture required to match acquisition speed.

WHO IS SHE BASH

- A Woman-Owned Small Business (WOSB) certified by the SBA — a comprehensive service and product development firm. Our mission: forge the connection between the standards-setting bodies in technology, from the open-source level to U.S. Government stakeholders, ensuring the security and durability of critical open-source infrastructure pivotal to national security.

WOSS | SBA Certified | Linux Foundation Member | Openset Member

Services for GovTech

- Zero Trust Network Architectures
- ICAM Strategy Analysis
- Identity, Credential & Access Management
- DevSecOps Design
- Engineering Services
- Open-Source Governance

The Platform: Dedzed

- An IL-5-ready DevSecOps platform deployed inside the government boundary — AWS GovCloud or on-prem. Not SaaS.

- Kasm VDI Workspaces
  - Secure, containerized browser-based developer workspaces executing safely inside the boundary.

- Command Dashboard
  - Centralized for real-time cost, system health, and secure, automated user/environment provisioning.

- Shredder Scanning Platform
  - Automated multi-engine security scanning, container hardening, and cryptographically verified SBOM generation.

- Ephemeral Environments
  - On-demand Kubernetes clusters provisioned dynamically per task and auto-destroyed to eliminate drift.

Ephemeral Environments, On Demand

- Policy driven cost-controlled environments
  - You are only charged for what you use (Short lived environments reduce cloud costs)
- Spin up per task. Tear down after
  - On-demand Kubernetes environments are provisioned for each task and destroyed when it ends
- Nothing left to drift
  - No persistent shared infrastructure means no drift from the accreditation baseline
- Provisioning becomes self-service
  - The provisioning bottleneck becomes a self-service action



Zero Trust Access

- Access is brokered per session, not per network

1 — Identity asserted
The session request authenticates to the broker, not to a network edge.

2 — Posture evaluated
User and device attributes are checked before any workspace exists.

3 — Policy decision
Authorization determines what this session is permitted to reach.

4 — Workspace instantiated
A Kasm container is provisioned inside the authorization boundary.

5 — Session destroyed
Workspace is torn down at session end. No persistent endpoint, no local data.

No VPN tunnel to a network, because there is no network to be on.

Designed against the DoD Zero Trust Strategy and Capability Execution Roadmap and NIST SP 800-207. Per-session brokering, device posture, and ephemeral workloads apply across the User, Device, Network, and Application and Workload pillars.

The Automated Pipeline

- On every build - not bolted on after

COMMIT — BUILD — RELEASE



GATE 1

Security Scanning

Integrated supply-chain and binary scanning via Shredder



GATE 2

SBOM

Software Bill of Materials generated on every build



GATE 3

CBOM

Cryptographic Bill of Materials generated on every build



GATE 4

Attestation

Signed provenance for each artifact, verifiable downstream

- Gate failure blocks promotion - no artifact reaches release without all four passing

Key Takeaways: The Dedzed Impact

- **A “Front Door” for Innovation**
  - Accelerator discovery now has somewhere to land. A small business finishing an 8-week cohort can be inside an accredited enclave rather than stopping at a pitch.
- **We Evaluate Code, Not Claims**
  - Assessment moves from reviewing slides to running software against mission-representative conditions, with verifiable scan results (SBOM/CBOM) produced on every build.
- **Informed Investment Decisions**
  - "Try Before You Buy.“ Funding decisions will now be made on demonstrated performance, not on vendor assertions.
- **Future-Proofing the Enterprise:**
  - Dedzed is more than a platform; it's a strategic capability that provides a persistent, secure, and repeatable way to evaluate and adopt the next generation of digital technologies.



QUESTIONS