



207 Big Springs Avenue
Tullahoma, TN 37388
(931) 455-2617

Proud to be 100% Employee Owned

www.microcraft.aero

Cyber Panel

NDIA Munitions Executive Summit 2019



Dr. Kenneth W. Sullivan, P.E.
President/CEO

NDIA Manufacturing Division Chairman
April 3, 2019

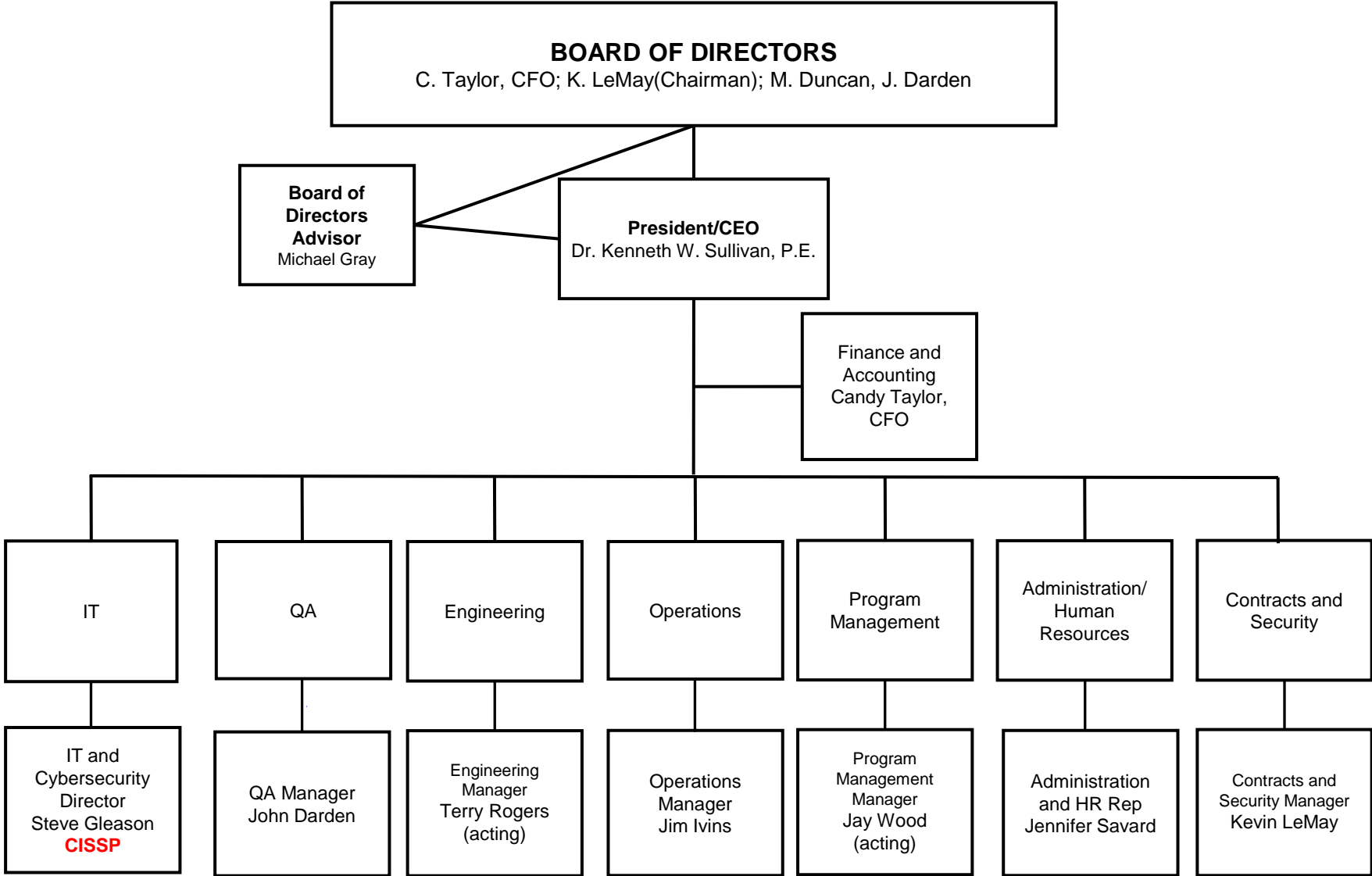
“Micro Craft is the “Go To Partner” for tough challenges in creating the Future of Flight and sustaining existing capabilities for Aerospace, Defense and Commercial customers while creating value for our stakeholders.”

Organization Chart



Proud to be 100% Employee Owned

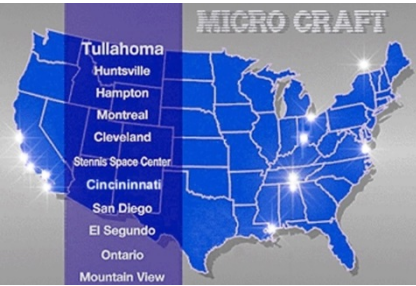
MICRO CRAFT, INC. (100% Employee Owned)



Sixty-Year Timeline

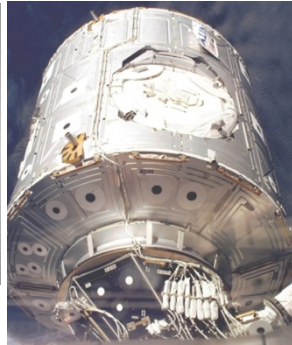


Proud to be 100% Employee Owned



Rapid expansion Begins

Pioneers in CNC, EDM, etc.



Space & Technology markets develop



NASA X-43 Hypersonic Flight Vehicles Manufacturer & Integrator

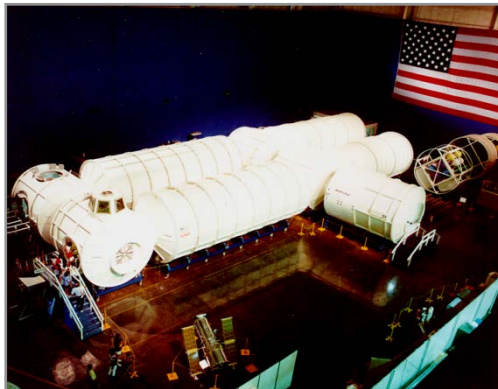
Hypersonic Engines Fabrication

Hypersonic Test Facility Hardware Upgrades for UTSI and AEDC

Key provider of complex wind tunnel models and other specialty test and flight hardware

1958 1985 1990 1996 2003 2011 2018

Founded by craftsman Charles Folk in Tullahoma Tennessee



Space Station Mock-Ups

NASA's Prime Contractor for the Hyper-X Program

After a brief period of ownership by an investment group, Micro Craft was acquired by ATK

Micro Craft was acquired by its employees

Meet the Owners ...

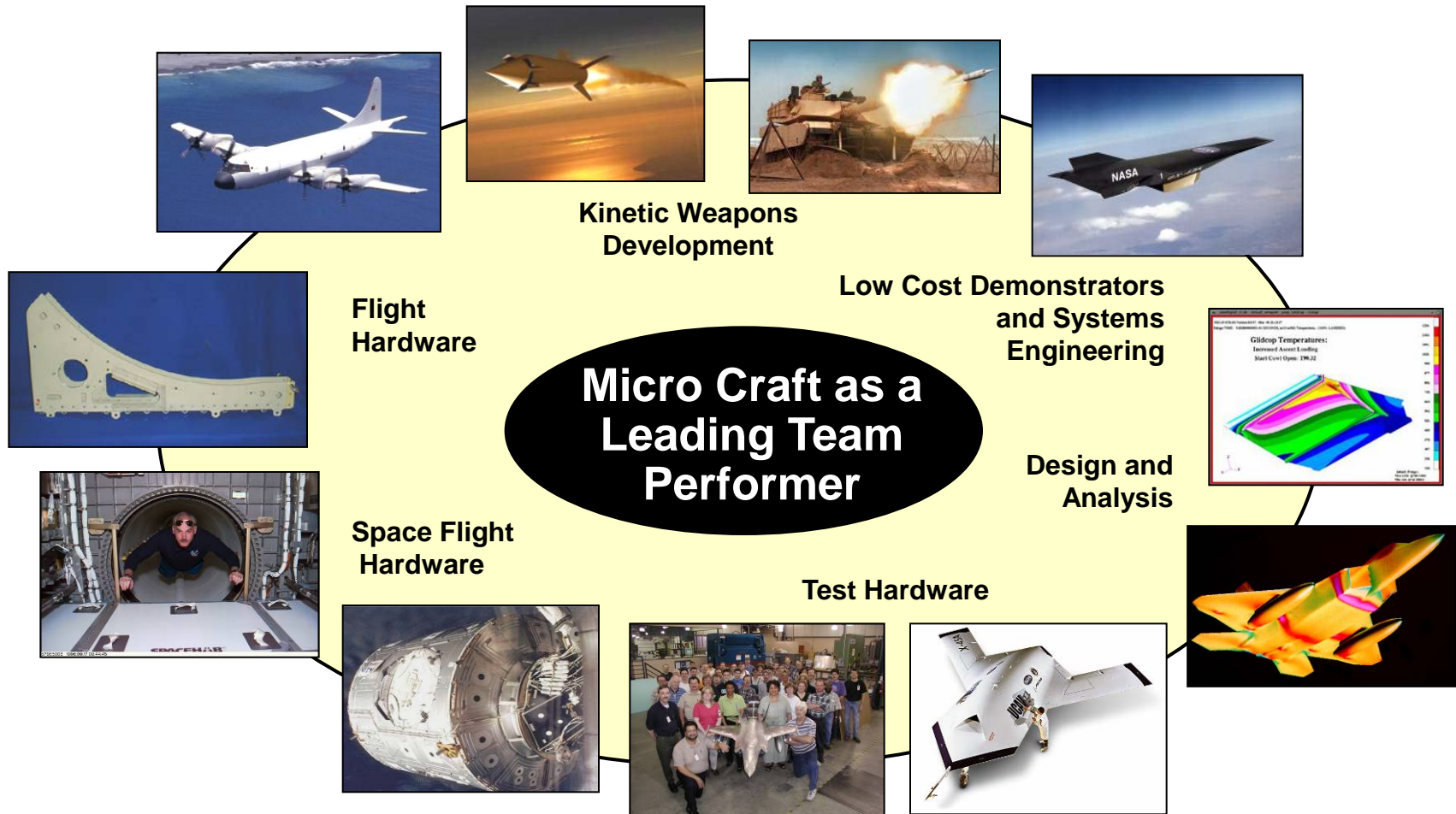


100% Employee-owned Small Business

Past Performance- Leading Edge Support



Proud to be 100% Employee Owned



Development, Engineer, Test, and Manufacture

What makes Micro Craft Different?



Proud to be 100% Employee Owned

- 1. Provides facility that has secure engineering and manufacturing capability.**
- 2. Micro Craft operates to a Quality Management System certified to AS9100D (technically equivalent to prEN9100:2016) and ISO 9001:2015 and is assessed in accordance with AS9104/1 for Research, Design, Development, Manufacture, Integration and Testing of Advanced Aerospace and Industrial Systems. Audited by third party Registrar BSI, ANAB accredited.**
- 3. Broad customer base that requires Micro Craft to support “one of a kind” to high production, mix model manufacture in a firm-fixed price (predominately) and cost-plus fixed fee R & D and production markets.**
- 4. Aggressively implementing (“baking in”) Cybersecurity requirements (NIST 800-171) in business processes and management systems. Participating in MANTECH Securing American Manufacturing.**

- **Used assessment tool (Imprimis I2ACT- 800 & CSET) to document as you continue to assess and implement**
- **Physical network segmentation**
 - Infrastructure in place: wiring, server and desktop hardware in place
 - Conducting phased testing
- **Applying “baked-in security” principals to:**
 - Business management process – focus on seamless adaptation
 - Lean process improvement projects (Value Stream Mapping)
 - Business management software development
- **“Securing American Manufacturing” Partner**
 - ManTech, LANL and Oak Ridge (Y12) cybersecurity initiative
 - Serving as a test bed model for security assessments
 - Participating in potential penetration testing to demonstrate program effectiveness

- **“Implementing Cybersecurity in the DoD Supply Chains”**
- **Published July 2018**
- **Located on NDIA website (Manufacturing Division/Resources)**
- **Based on survey of NDIA Manufacturing Division members**

- **Overall, respondents had an uneven awareness of cybersecurity: they appreciated the need for protection of IT/IP; there was far less support for operational aspects.**
- **Most small- to medium-sized (SME) suppliers have a poor understanding of cybersecurity.**
- **Understanding of both the mandatory DFARS requirements and the underlying NIST framework are limited.**
- **Most firms in the early stages of implementation severely underestimate the costs of becoming compliant by as much as a factor of 10.**
- **Respondents see the DFARS requirements not as something that is economically justified but rather as a cost of doing business (along with all that this view brings).**

For the Federal government:

- Develop awareness that cybersecurity is both a national and economic security issue within the supply chain.
- Help simplify the process of meeting the new DFARS requirement.
- Develop a certification program focusing on supply chain cybersecurity.

For Prime Contractors:

- Help develop a compelling business case for cybersecurity.
- Help the SMEs by developing and using appropriate measures of cybersecurity.
- Treat SME suppliers appropriately, as to whether they are early or late adopters by rewarding proactive implementation.

For Small/Medium Sized Suppliers

- Focus on improving knowledge and awareness regarding cybersecurity.
- Understand that cybersecurity is now a cost of doing business in today's cyber/digital market.
- Understand that cybersecurity is a corporate responsibility – one that cannot be subcontracted.

- **This DFAR requirement has the potential to negatively impact the DoD Industrial Base**
 - Interpretation
 - How are suppliers certified?
 - Suppliers whose minority business base is DoD/Government may “walk away” due to impact on overhead cost and their ability to compete in a commercial market
 - Companies that perform classified work should have an easier time understanding and implementing the DFAR 800-171.
- **Opportunity for “cabin industries” to “help” SMEs with their compliance**
- **Cyber is a 24/7/365 activity**



Proud to be 100% Employee Owned

Questions?