Emerging Technology Ventures, Inc.
Company Update

Presented For:

Sustainability Manufacturing Day

July 20th, 2022

Agenda:

- Cyber Security Update
  - Controlled Unclassified Information (CUI)
  - NIST Special Publications
  - Department of Defense Cybersecurity Maturity Model Certification
- MEP Grant Support
- Our Navy Customer
- Building a Sustainable Workforce through Interns and Employee Growth
- Wrap up

Definitions

- **Controlled Unclassified Information (CUI)** is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
- **NIST Special Publication (SP)800-171** or just 800-171 is a codification of the requirements that any non-Federal computer system must follow in order to store, process, or transmit Controlled Unclassified Information (CUI) or provide security protection for such systems.
- **The Cybersecurity Maturity Model Certification (CMMC)** is the Department of Defense's (DoD) newest verification mechanism designed to ensure that cybersecurity controls and processes adequately protect Controlled Unclassified Information (CUI) that resides on Defense Industrial Base (DIB) systems and networks.

Requirements for Handling CUI

NIST SP 800-171:

- 3.1.1/3.1.2 Access Control - Limit information system access
- 3.1.20/3.1.22 Verify/control connections from external systems
- 3.5.1/3.5.2 Authenticate users as prerequisite to allowing access
- 3.13.1/3.13.5 Implement subnetworks for public access that physically or logically separated from internal network
- 3.14.3 Monitor system security alerts and take action in response

DoD CMMC Level 1:

- AC.1.001, AC.1.002: Access Control - Limit information system access
- AC.1.003, AC.1.004: Verify/control connections from external systems
- IA.1.076, IA.1.077: Authenticate users as prerequisite to allowing access
- SC.1.175, SC.1.176: Implement subnetworks for public access that physically or logically separated from internal network
- SI.2.214: Monitor system security alerts and take action in response

Scope of MEP Grant

Tularosa Communications Inc. (TCI) provided:

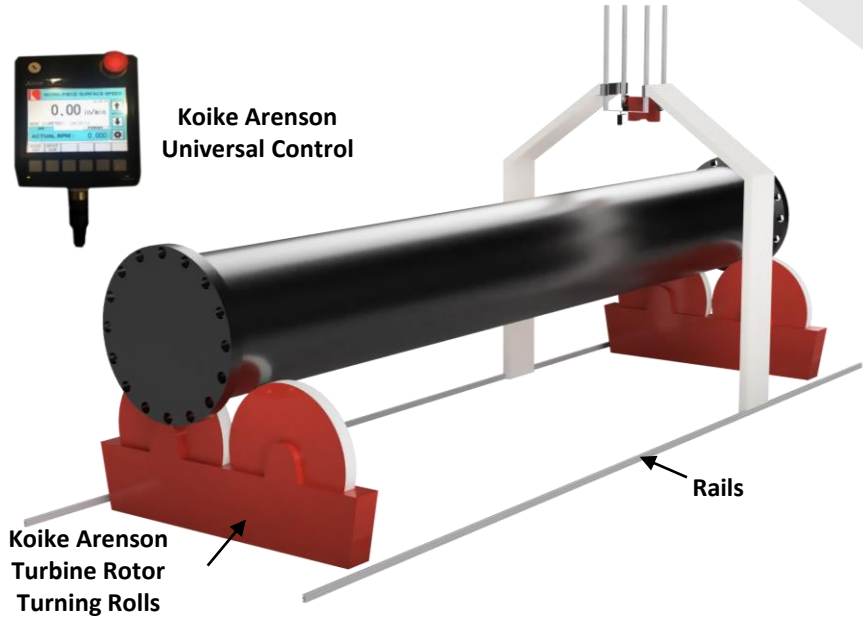
- **Created guest wireless network separate from internal company LAN**.
  - Covers - 3.13.1/3.13.5 Implement subnetworks for public access that physically or logically separated from internal network and SC.1.175, SC.1.176
- **Enabled Multi-Factor Authentication (MFA) and Least Privilege security settings for all accounts in Microsoft 365**
  - Covers - 3.1.1/3.1.2 Access Control - Limit information system access and AC.1.001, AC.1.002
- **Configured and implemented VPN and Local MFA**
  - Covers 3.5.1/3.5.2 Authenticate users as prerequisite to allowing access and IA.1.076, IA.1.077

Immediate Impact with our Navy Customer

- The US Navy has currently tasked us to create a system for Autonomous Inspection of Large Marine Shafts
- The data that will be transmitted from the Navy Shipyards to us and vice versa, could contain Controlled Unclassified Information (CUI) (such as inspection data, serial numbers, vessel names that are out of commission) that must be protected when in transit and at rest within our Information System.
- Our Information System is now capable of protecting this data.
- With this system configuration, all our employees will be able to securely access the data even if they are off-site, effectively increasing productivity.

System Level Overview

- Builds 3D Digital Twin from as-built drawings
- Utilizes existing infrastructure platforms w/ automated gantry (rail or overhead) for scanning
- Able to move between workstations for optimization
- Integrated w/platform controller for rotation
- Preprogrammed inspection sequence by serial number
- Utilizes existing inspection workflow to facilitate transition between autonomous and manual
- Camera/Laser scanner uses photogrammetry to update 3D Digital Twin with anomalies creating 4D Digital Twin (4th D = Time)
  - Layered visualization to view previous anomalies/repairs
- Flange sensor head (camera/ultrasound) for inspection



Examples of Shafts Under Inspection

Employee/Intern Update:

Many of our interns return after internship to become full-time employees.

Here are just two examples:

Nick Brinegar

- Started as an intern June of 2020 and continued while still attending high school.
- Lead CAD Technician
  - Designed the structure of the shaft inspection platform for the Navy application.
- Lead Additive Manufacturing Technician
- Member of the Design & Testing group for our platform prototypes.
- Starts NMSU in the fall going for his Mechanical Engineering degree.
  - Will continue to work with ETV on the Navy project.

Jordan Gonzalez

- Started with ETV as an intern in 2016 while still attending high school under the Workforce Innovation and Opportunity Act.
- Started working full time after high school graduation in 2017.
- Currently attending CNM online for his IT Support Specialist Certification under the New Mexico Information Technology Apprenticeship Program as a growth opportunity.

Wrap Up

Thanks to the New Mexico MEP for investing in ETV!

With the assistance of the MEP program:

- Our Information System:
  - is more secure than it has ever been
  - is ready to protect data weeks ahead of schedule
  - is much easier to access by our off-site employees
- We now meet critical NIST SP 800-171 and CMMC Level 1 requirements for supporting our Federal partners including DoD and NASA