MEP Program Grant Update
Impact on Emerging Technology Ventures
Attaining Compliance with NIST SP-800-171

Presented To:

Denise Williams (Monaghan)
Innovation Director Four Corners New Mexico
New Mexico Manufacturing Extension Partnership (MEP)
San Juan College
Farmington, New Mexico

June 9th, 2022

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

Solution

- Cisco Meraki and Microsoft 365 E5 were chosen because they support:
  - On-site access for employees (managed desktop)
  - Secure, remote access for offsite employees and collaborators (Alamogordo, Las Cruces, Socorro, and Crownpoint, NM; Indiana; Hawaii)
  - Secure data transfer with suppliers and customers
- Managed Service Provider (MSP) - Tularosa Communications Inc. (TCI)
- In addition to the $8000 services funding from the MEP program, ETV has spent more than $10,000 for hardware and licenses setting up the system

Scope of MEP Grant

Tularosa Communications Inc. (TCI) provided:

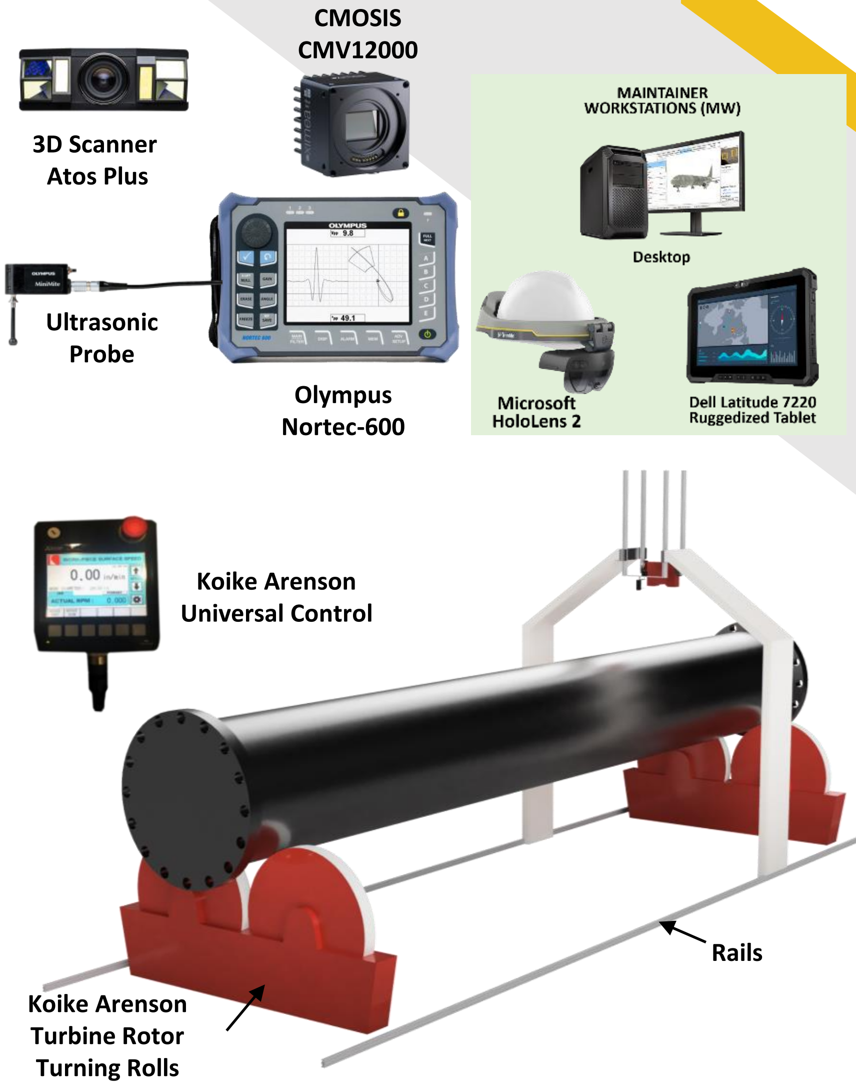
- **Created guest wireless network separate from internal company LAN**.
  - Covers - 3.13.1/3.13.5 Implement subnetworks for public access that physically or logically separated from internal network and SC.1.175, SC.1.176
- **Enabled Multi-Factor Authentication (MFA) and Least Privilege security settings 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

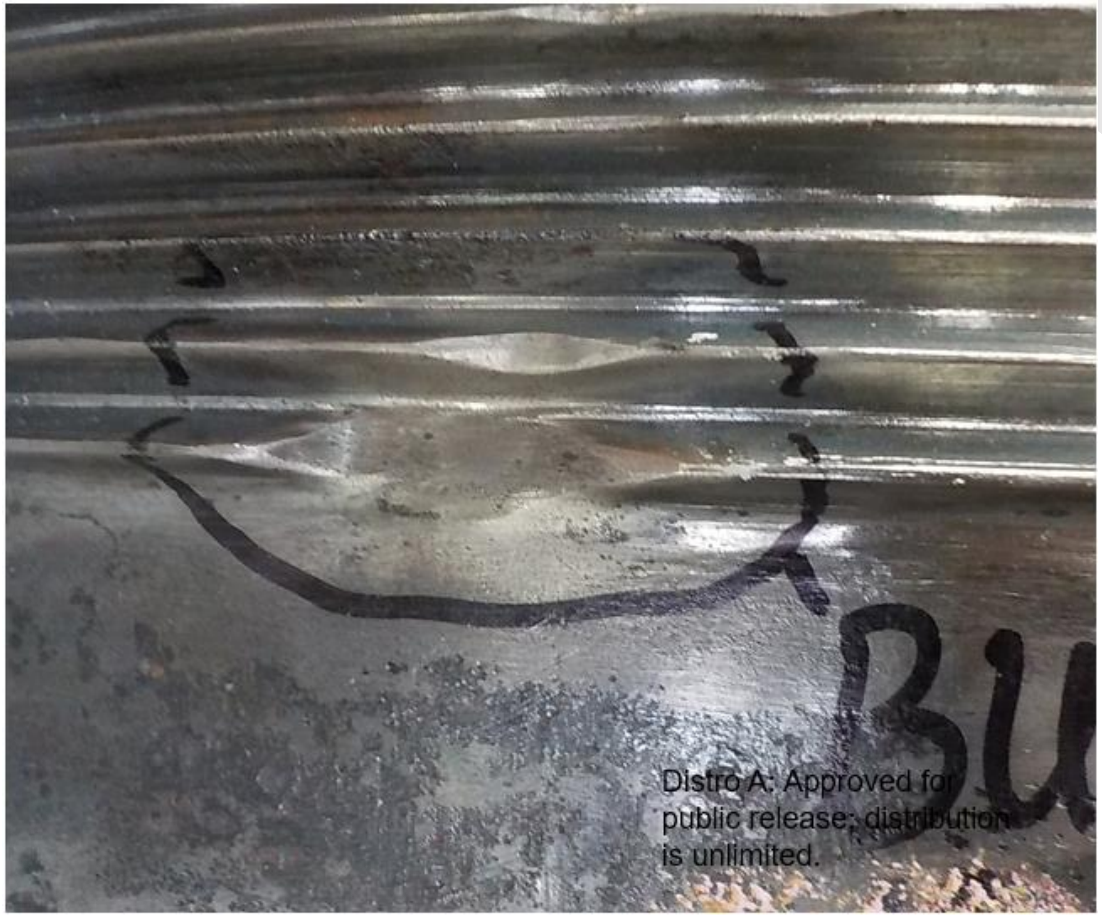
- Builds 3D Digital Twin from as-built drawings
- Utilizes existing infrastructure platforms w/ automated gantry (rail or overhead) for scanning
- Able to move between workstations for optimization
- Integrated w/platform controller for rotation
- Preprogrammed inspection sequence by serial number
- 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

Distro A: Approved for public release; distribution is unlimited.

Distro A: Approved for public release; distribution is unlimited.



Distro A: Approved for public release; distribution is unlimited.

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