Cyber DFAR Summit 2016
Small Business Experience –
Lesson’s Learned

Mr. Steve Gleason, CISSP
December 7, 2016
Micro Craft History

• Founded in 1958 by craftsman Charles Folk
• Key provider of complex wind tunnel models and other specialty hardware – pioneers in CNC, EDM, etc.
• Rapid expansion in 1990s into space and technology markets
• Prime contractor and vehicle manufacturer and integrator for NASA’s X-43A and X-43C Hyper-X Programs
• After a brief period of ownership by an investment group, Micro Craft was acquired by ATK in 2003.
• In 2011, Micro Craft was acquired by its employees and became a **100% Employee-owned Small Business**.
Micro Craft Core Competencies

Proud to be 100% Employee Owned

Development, Engineer, Test, and Manufacture
Manufacturing Capabilities

- Celebrating 50+ years of experience in providing precision manufacturing to NASA, DoD, and OEMs

- Manufacturing
  - 57,000 sq. ft. facility
  - 3-, 4-, and 5-axis milling
  - Large CNC lathe machining
  - Wire EDM, die sink EDM
  - ID/OD grinding
  - Metals, composites, ceramics, and exotic metals
  - Complex components, assemblies and integrated systems
  - Prototype research hardware
  - Electronics Lab and cable harness facilities

- Quality
  - 2005 Comet Award for Excellence in Manufacturing
  - DPD (Digital Product Definition) and MBD (Model Base Definition) Boeing Certified
  - Lockheed Martin Quality Select Supplier
  - NASA Small Business Contractor of the Year
What makes Micro Craft Different?

1. Provides secure facility that has classified engineering and manufacturing capability

2. Quality department in place to support critical and complex aerospace hardware component manufacture

3. Broad customer base that requires Micro Craft to support “one of a kind” to high production, mix model manufacture in firm-fixed price and cost-plus fixed fee competitive R & D and flight hardware markets

4. Aggressively implementing (“baking in”) Cybersecurity requirements in business processes and management systems while implementing lean process principles to stay competitive and compliant
Cyber security has come to depict a range of nefarious computer break-ins by shadowy hackers with cryptic names that compromise the credit card accounts of retail store patrons, emails by notable politicians, and the control of cars and unmanned aircraft.

As regulations have emerged, federal contractors have been given ambiguous direction regarding achieving compliance. December 31, 2017 is the drop dead date. Many cybersecurity product and service providers display a minute by minute count down on their websites, attempting to accelerate the purchase of mitigation products base on fear.

- **THREATS AND VULNERABILITIES ARE REAL AND INCALCULABLE**

- **COMPLY OR DIE**
Micro Craft Environment

- 60+ employees, 40 of which are owners

- Manufacturing Craftsmen and CNC operators, Manufacturing Management, Engineers, Estimators, Accounting, Contracts, Security, IT, Business Development, Executive Management

- Unclassified and Classified Programs

- Network
  - 75 workstations
  - 10 servers
  - Wireless guest and internal access
  - CNC controllers
  - Firewall
  - Tablets, Smart Phones
Network Design

Proud to be 100% Employee Owned

Server Room

- Default VLAN: 192.168.200.1
- X0.V2: 10.10.40.1 Management
- X0.V3: 10.10.53.1 Internal - Wifi
- X0.V4: 10.10.54.1 Guest - Wifi
- X0.V5: 10.10.55.1 Internal - Wifi - 5Ghz
- X0.V6: 10.10.56.1 Guest - Wifi - 5Ghz
- X0.V7: 10.10.57.1 SonicPoints
- X0.V8: 10.10.41.1 Server Management

Shop (Wall Mounted)

- MCI - SW - 3
  - HP - 1910
  - 10.10.40.13

- MCI - SW - 4
  - HP - 1910
  - 10.10.40.14

- MCI - AP - 1
  - Sonicpoint

- MCI - SW - 5
  - HP - 1810
  - 10.10.40.15

- MCI - NAS - 1
  - 192.168.200.130

- MCI - ESXi - 1
  - 192.168.200.51

- MCI - ESXi - 2
  - 192.168.200.52

- MCI - ESXi - 3
  - 192.168.200.53

- LACP (4 Lines)

- (VLAN Trunk)

- Data Diode

- 10.10.60.1 Air Gap Subnet (Blocked at Firewall)

- (VLAN Trunk) Redundant 2 Lines

- (VLAN Trunk)

- Only For Management

- 10.10.40.11

- 196.109.1

- MCI - FW - MAIN
  - Sonicwall 2600
Rapid Security/Control Assessment

- **Categorize**
  - Administrative
  - Physical
  - Technical

- **Inventory**
  - Compliant
  - Partial
  - No
  - N/A

- **Prioritize**
  - Risk to Assets
  - Cost of Acquisition
  - Ease of Implementation
Get to Work

• Implement each control based on priority of safeguarding data

• Identify low hanging fruit along the way
  • Administrative (upgrade/”tweak” existing systems)
  • Review/”Lean-out” business processes

• Prepare and respond to control impact on users
  • Supporting users in a small business is a unique challenge
  • Attitudes toward new security controls will not change over night
  • Regular group communication either through email or formal training sessions is critical to timely implementation of security controls.
  • Most small business users wear multiple hats
  • Controls will expose processes that must be altered and improved (document)

• Use assessment tool
Self Assessment - Evidence

Evaluate Compliance (NIST 800-171)

<table>
<thead>
<tr>
<th>Number</th>
<th>Family</th>
<th>Basic/Derived</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>ACCESS CONTROL</td>
<td>Basic</td>
</tr>
</tbody>
</table>

Requirement: Employ the principle of least privilege, including for specific security functions and privileged accounts.

Suggested Evidence: 800-53 References, Special Guidance, Questions, Remediation Action

SUGGESTED EVIDENCE: Access Control Policy, copy of group access structure, privileged user agreements.

POTENTIAL ASSESSMENT METHODS AND OBJECTIVES (Derived from 800-53A):
EXAMINE: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; information system audit records; list of system-generated privileged accounts; list of system administration personnel; other relevant documents or records
INTERVIEW: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; system/network administrators; organizational personnel with information security responsibilities;
TEST: Automated mechanisms implementing least privilege functions.

Eval By: 
Date: 

Comply 0 Partial 0 No 0 N/A 0 No Response 109
Source: 800-171 R, FAR 15
Filter: 

[© 2014-2016 Imprimis Inc.]
Evaluate Compliance (NIST 800-171)

Go to Family: ACCESS CONTROL  Number: 

Filter For Only: 
- Comply
- Partial
- No
- N/A
- No Response

3.1.1 ACCESS CONTROL  Basic

Requirement: Employ the principle of least privilege, including for specific security functions and privileged accounts.

Suggested Evidence: 800-53 References  Special Guidance

AC-02-00  Account Management
The organization:
a. Identifies and selects the following types of information system accounts to support organizational missions/business functions:
Assignment: organization-defined information system account types;

AC-03-00  Access Enforcement
The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Eval By: 
Date: 
Compliant  Partial  No  N/A  No Response

Source: 800-171 R, FAR 15
Filter: 

© 2014-2016 Imprimis Inc.
Evaluate Compliance (NIST 800-171)

Requirement: Employ the principle of least privilege, including for specific security functions and privileged accounts.

Suggested Evidence: 800-53 References, Special Guidance, Questions, Remediation Action

Eval By: [Field]
Date: [Field]
Comply: 0
Partial: 0
No: 0
N/A: 0
No Response: 0
Source: 800-171 R, FAR 15
Filter: [Field]

[© 2014-2016 Imprimis Inc.]
Self Assessment - Remediation
Self Assessment - Remediation Report

Summary
This assessment was accomplished between 7/27/2016 and 8/10/2016. Assessment done by: Carol Jones, ISRM, D. Warbucks, CIO, Steve Johnson, FSS, T. Assessment done on 128 requirements, based on NIST 800-171 CUI Controls, NIST 800-171 Requirements, FAR 15-600-171 Equivalents.

Compliant
- Partial
- No Compliance
- Not Applicable

NIST 800-171 Requirements
- No Compliance
- Partial
- No

No Compliance (2)

Requirement: Alert in the event of an audit process failure.

Assessment Comments:
Does the failure of any audit process generate an alert?

Question:
- Does your organization have a policy for responding to an audit process alert?

Remediation:
Entry in remediation for 3.1.14


Action Detail:
- Encrypt UI on mobile devices.

Number in category noted at beginning
Number in category noted at end

Summary highlights challenges

All sections selected

Only Remediation section selected
<table>
<thead>
<tr>
<th>Requirement/Control</th>
<th>Assessment</th>
<th>Remediation Title</th>
<th>Start Date</th>
<th>Finish Date</th>
<th>Notes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Date Evaluated</th>
<th>Evaluated By</th>
<th>Attachments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/8/2016</td>
<td>Carol Jones, ISM</td>
<td>0</td>
</tr>
<tr>
<td>2/2/2016</td>
<td>Ted Baxter, IT manager</td>
<td>0</td>
</tr>
<tr>
<td>1/30/2016</td>
<td>Ted Baxter, IT manager</td>
<td>0</td>
</tr>
<tr>
<td>2/3/2016</td>
<td>D. Warbucks, CIO</td>
<td>0</td>
</tr>
<tr>
<td>2/8/2016</td>
<td>Carol Jones, ISM</td>
<td>0</td>
</tr>
</tbody>
</table>
Self Assessment Tool Tips

- Gather all existing policy and procedure documents

- Utilize policy and form templates and attach to each control

- If possible to divide and conquer by delegating policy gathering and creation

- Don’t hesitate to mark No upon first pass evaluation. Progress through the questions as quickly as possible.

- The SSP and POAM are the most important documents produced in IS accreditation.
Path Forward

• 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
  • Developing metrics for continuous monitoring and supply chain monitoring
  • Lean process improvement projects
  • 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
  • Participated in first assessment with Y12 at the end of October
  • Future penetration testing to demonstrate program effectiveness
Questions?