Micro Craft, Inc.
NDIA Procurement Division
Cyber DFARS Workshop

Mr. Steve Gleason, CISSP
January 9, 2018
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

Micro Craft Core Competencies

Kinetic Weapons Development

Low Cost Demonstrators and Systems Engineering

Design and Analysis

Development, Engineer, Test, and Manufacture
Company

- 60+ employees, 40 of which are owners
- Manufacturing Craftsmen and CNC operators, Manufacturing Management, Engineers, Estimators, Accounting, Contracts, Security, IT, Business Development, Executive Management

Business Base

- DoD classified and unclassified programs
- Commercial projects

Information System / Data

- On-premise servers and workstations
- Virtual server farm
- Variety of workstation classes
- Engineering and design technical data
Assessment Process

- Assess
- Develop & Update
- Monitor
- Plans of Action

Security Assessment Process
Compliance Team

- CEO
- HR
- FSO
- Contracts
- CIO
Continuous Assessment Flow

Begin Assessment

Select Beginning Baseline

Tailor and Modification

Determine Control Category

End Assessment

Document Remediation Requirements & Recommendations

Generate Report

Step through Each Control: Determine Compliance, Document

Remediate

Update Documentation

Archive Assessment Data

Maintain Compliance Profile
### Controls Inventory

#### Crosswalk 800-171 to 800-53

<table>
<thead>
<tr>
<th>AT-3</th>
<th>Role-Based Security Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl ID</td>
<td>AT-3</td>
</tr>
<tr>
<td>Ctrl Text</td>
<td>The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. At least annually thereafter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AT-2(2)</th>
<th>INSIDER THREAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl ID</td>
<td>AT-2(2)</td>
</tr>
<tr>
<td>Ctrl Title: INSIDER THREAT</td>
<td></td>
</tr>
<tr>
<td>Ctrl Text</td>
<td>The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.</td>
</tr>
</tbody>
</table>
Evaluate Compliance (NIST 800-171)

Go to Family: ACCESS CONTROL

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
Evaluate Compliance (NIST 800-171)

3.1.1 ACCESS CONTROL

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

Suggested Evidence: 800-53 References

[Image of a self-assessment tool interface]
Summary
This assessment was accomplished on 5/30/2017
Assessment done by; Aaron Jones; Steve Gleason
Assessment done on 109 Requirements, based on NIST 800-171 Requirements, FAR 15 - 800-171 Equivalents

- Requirements Selected: 109
- Requirements Evaluated: 109
- No Response: 0

- Compliant: 102
- Partial: 4
- No Compliance: 1
- Not Applicable: 2
- No Response: 0

Approximately 95% Complete
Compliance Documentation

- SSP – System Security Plan
- POA&M – Plan of Actions and Milestones

![System Security Plan](image1.png)

**Plan of Action and Milestones (POA&M)**

- **System Name**: Micro Craft, Inc. Network
- **Company/Organization Name**: Micro Craft, Inc.
- **POC**: John Smith, 911-455-2800, ext. 466, john.smith@microcraft.com
- **S Type**: Local Area Network

<table>
<thead>
<tr>
<th>D</th>
<th>Weakness or Deficiency</th>
<th>Security Control</th>
<th>POC</th>
<th>Resources Required</th>
<th>Scheduled Completion Date</th>
<th>Weakness/Deficiency Identified by</th>
<th>Risk Level</th>
<th>Estimated Cost</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Develop formal quarterly awareness training, seek web-based solution</td>
<td>3.2.3</td>
<td>John Smith</td>
<td>Overhead Labor</td>
<td>3/31/2018</td>
<td>John Smith</td>
<td>Medium</td>
<td>$500.00</td>
<td>Planned</td>
</tr>
<tr>
<td>2</td>
<td>Develop and test incident response plan</td>
<td>3.6.3</td>
<td>John Smith</td>
<td>Overhead Labor</td>
<td>6/31/2018</td>
<td>John Smith</td>
<td>Medium</td>
<td>$7,500.00</td>
<td>Planned</td>
</tr>
</tbody>
</table>
A document that describes how a small manufacturer meets the security requirements for a system or how a small manufacturer plans to meet the requirements.

The system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.
What are Plans of Action?

Describes how many unimplemented security requirements will be met and how any planned mitigations will be implemented. Companies can document the system security plan and plan of action as separate or combined documents and in any chosen format.

When requested, the System Security plan and any associated Plans of Action for any planned implementations or mitigations should be submitted.
Implementation of SSP

Resulting Documentation

• Departmental Interviews
• Gather Existing Policies and Procedures
• Create Policies and Procedures
• Awareness and Training

Technologies to meet controls

• Vulnerability Scanning
• Patch Management
• Endpoint Management
• Firewall Configuration
• Group Policies
Assessment / Implementation Notes

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

• Prepare and respond to control’s 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 are 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)
Supporting Implementation Activities

- Continuous Monitoring Plan
- Breach Recovery Plan
- Automation
- MEP Involvement at the National and State Level
- Penetration Testing – UpTech Services, Shelbyville Tech
- Continuous evaluation of risk (threats, vulnerabilities…)
- Participation in Y-12, Man Tech, Securing American Manufacturing Program
- Security Technology Projects – Blockchain
Future Challenges and Direction

- Flow Down / Supply-chain accountability
- Need built-in incentives to maintain strong cyber posture
- Growing Cyber Threats – *(Spear Fishing 80%)*
- Cloud Services Considerations
Questions?