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

Mr. Steve Gleason, CISSP
December 7, 2016

Micro Craft History

Proud to be 100% Employee Owned

- Founded in 1958 by craftsman Charles Folk

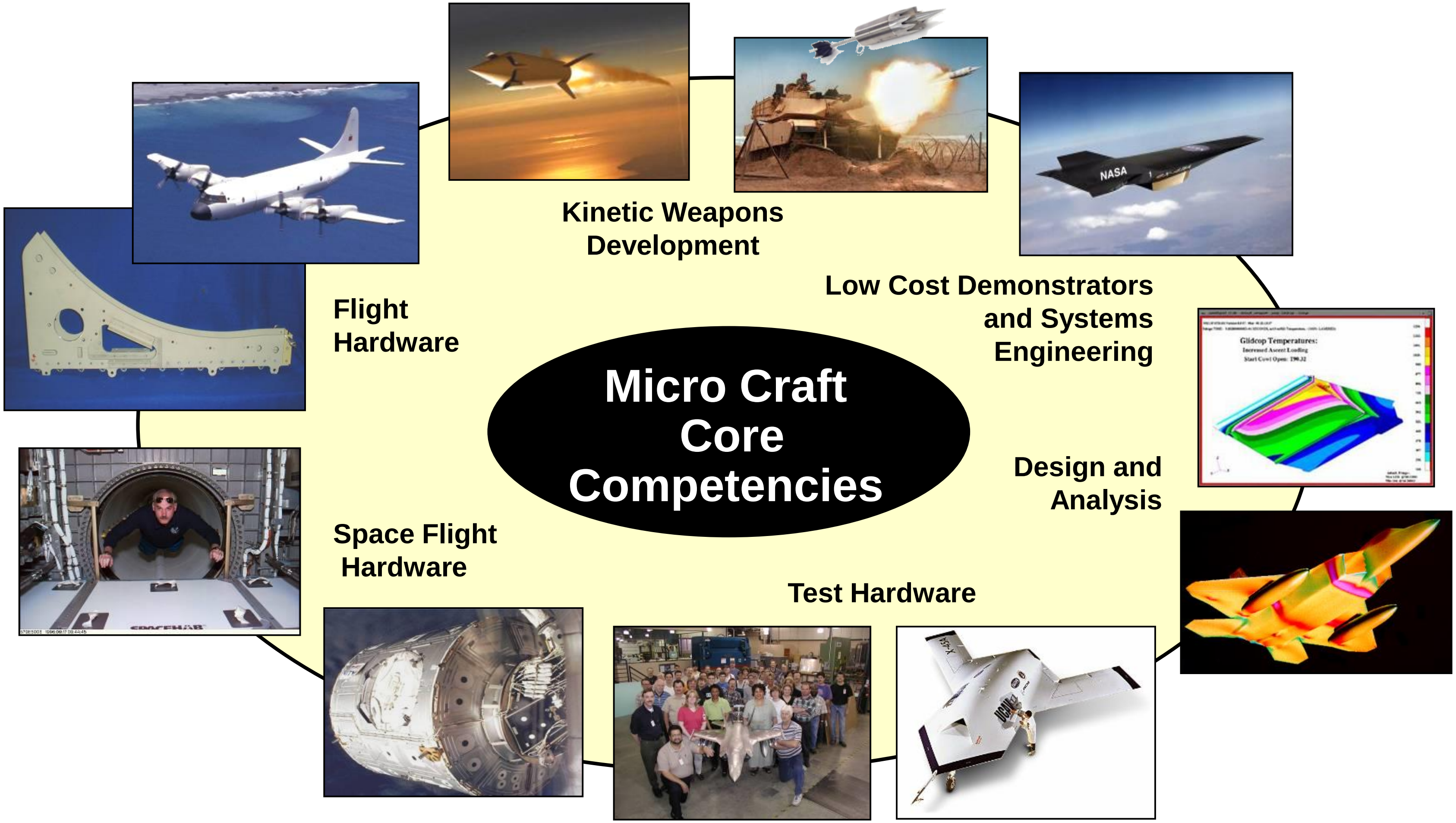
- Key provider of complex wind tunnel models and other specialty hardware – pioneers in CNC, EDM, etc.

- 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



Micro Craft Core Competencies

Kinetic Weapons Development

Low Cost Demonstrators and Systems Engineering

Design and Analysis

Test Hardware

Space Flight Hardware

Flight Hardware

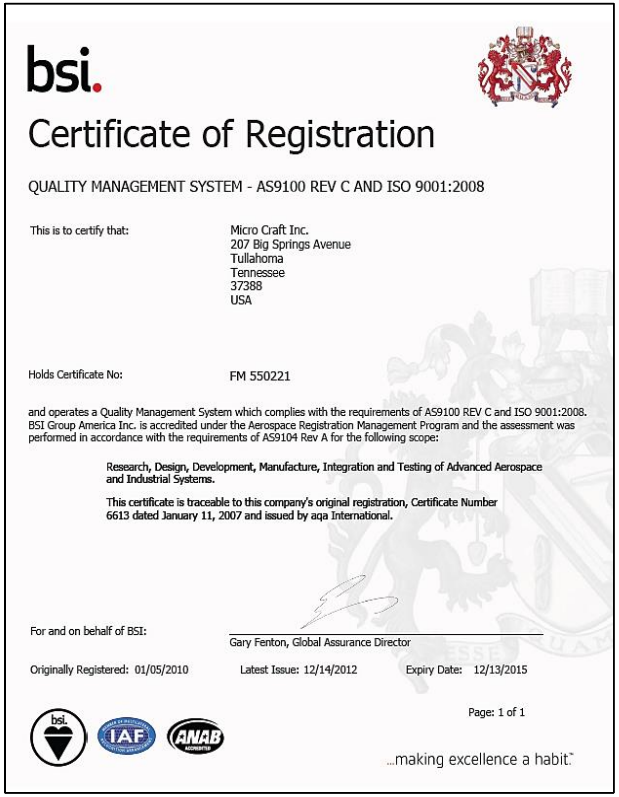
Development, Engineer, Test, and Manufacture

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**
  - AS 9100 Rev C and ISO 9001:2008 Certification
  - 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



bsi.

Certificate of Registration

QUALITY MANAGEMENT SYSTEM - AS9100 REV C AND ISO 9001:2008

This is to certify that:

Micro Craft Inc.
207 Big Springs Avenue
Tullahoma
Tennessee
37388
USA

Holds Certificate No: FM 550221

and operates a Quality Management System which complies with the requirements of AS9100 REV C and ISO 9001:2008. BSI Group America Inc. is accredited under the Aerospace Registration Management Program and the assessment was performed in accordance with the requirements of AS9104 Rev A for the following scope:

Research, Design, Development, Manufacture, Integration and Testing of Advanced Aerospace and Industrial Systems.

This certificate is traceable to this company's original registration, Certificate Number 6613 dated January 11, 2007 and issued by aqa International.

For and on behalf of BSI:

Gary Fenton, Global Assurance Director

Originally Registered: 01/05/2010 Latest Issue: 12/14/2012 Expiry Date: 12/13/2015

Page: 1 of 1

...making excellence a habit.™

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**

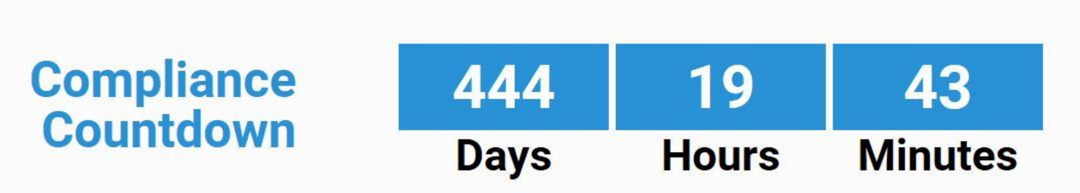
4. **Aggressively implementing ("baking in") Cybersecurity requirements in business processes and management systems while implementing lean process principles to stay competitive and compliant**

Cyber Security/Compliance Obscurity

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**



Compliance Countdown

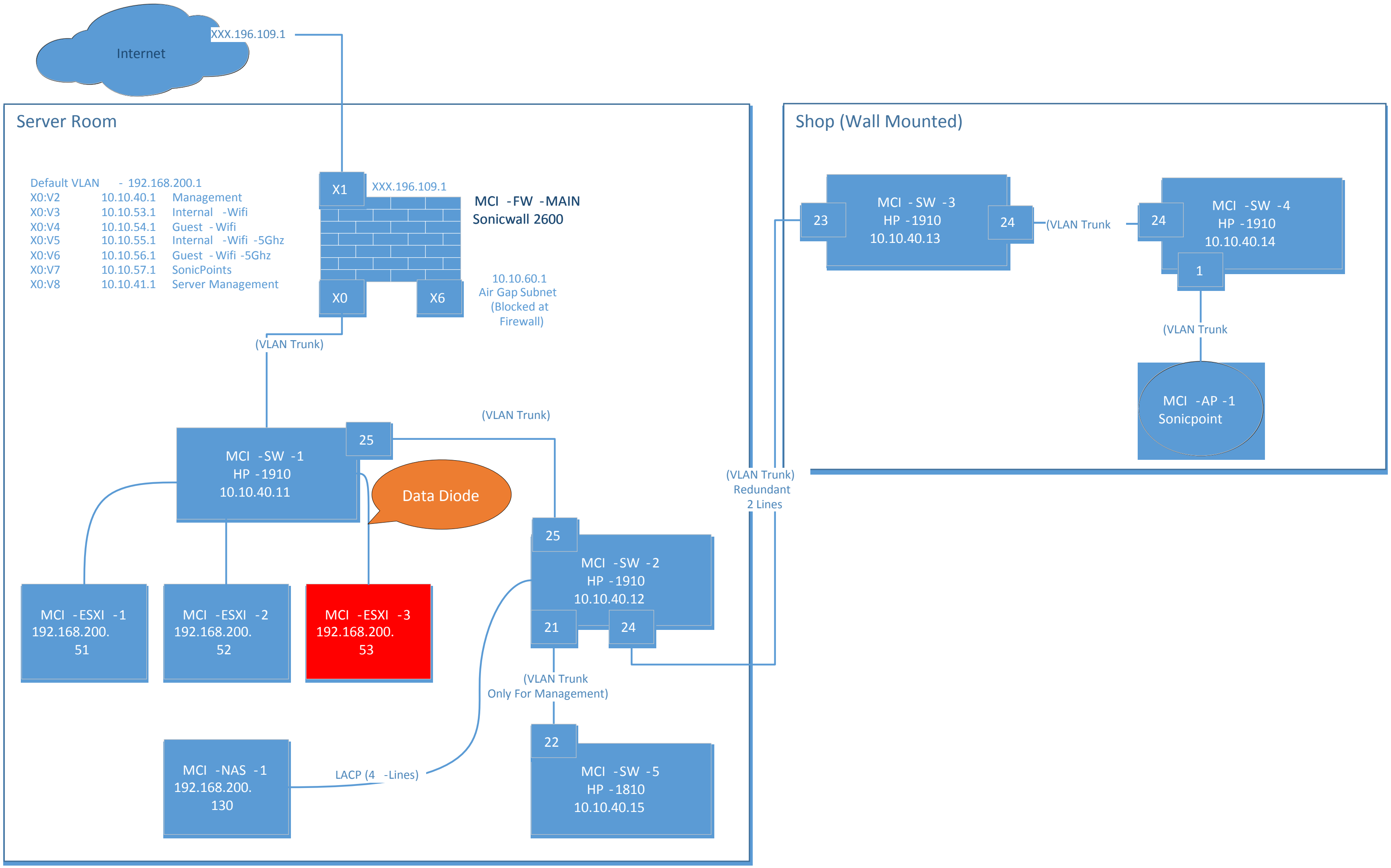
444	19	43
Days	Hours	Minutes

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



Internet

XXX.196.109.1

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

X1

XXX.196.109.1

MCI -FW -MAIN
Sonicwall 2600

X0

X6

10.10.60.1
Air Gap Subnet
(Blocked at
Firewall)

(VLAN Trunk)

25

MCI -SW -1
HP -1910
10.10.40.11

(VLAN Trunk)

Data Diode

MCI -ESXI -1
192.168.200.
51

MCI -ESXI -2
192.168.200.
52

MCI -ESXI -3
192.168.200.
53

25

MCI -SW -2
HP -1910
10.10.40.12

21

24

(VLAN Trunk
Only For Management)

22

MCI -SW -5
HP -1810
10.10.40.15

MCI -NAS -1
192.168.200.
130

LACP (4 -Lines)

(VLAN Trunk)
Redundant
2 Lines

Shop (Wall Mounted)

23

MCI - SW -3
HP -1910
10.10.40.13

24

(VLAN Trunk

24

MCI -SW -4
HP -1910
10.10.40.14

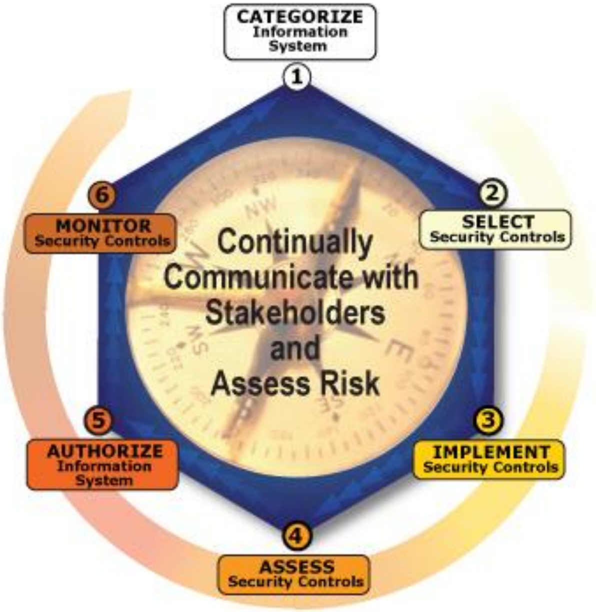
1

(VLAN Trunk

MCI -AP -1
Sonicpoint

Rapid Security/Control Assessment

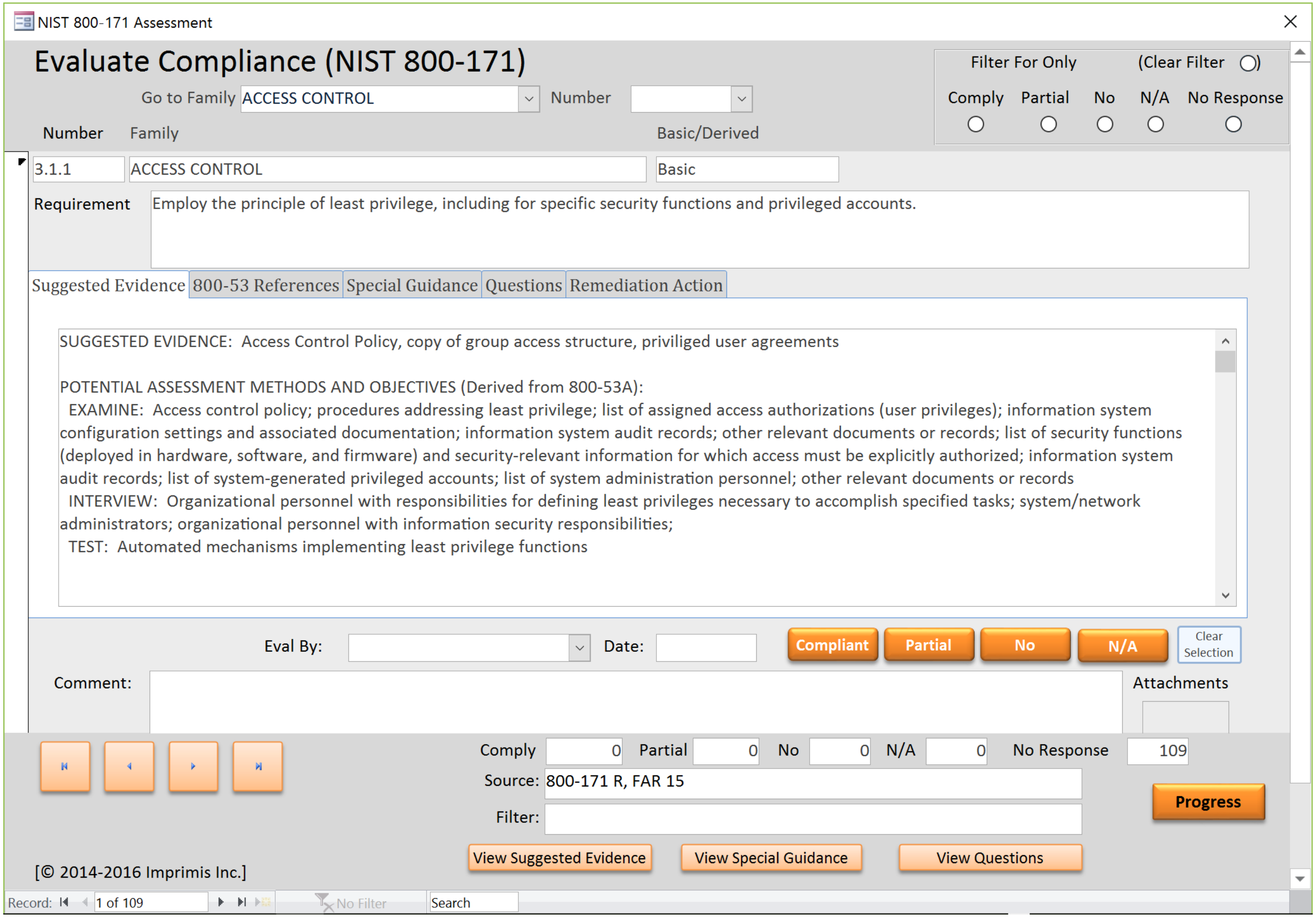
- **Categorize**
  - Administrative
  - Physical
  - Technical
- **Inventory**
  - Compliant
  - Partial
  - No
  - N/A
- **Prioritize**
  - Risk to Assets
  - Cost of Acquisition
  - Ease of Implementation


CATEGORIZE Information System
1
2
SELECT Security Controls
3
IMPLEMENT Security Controls
4
ASSESS Security Controls
5
AUTHORIZE Information System
6
MONITOR Security Controls
Continually Communicate with Stakeholders and Assess Risk

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



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family: ACCESS CONTROL

Number:

Filter For Only (Clear Filter ○)

Comply ○ Partial ○ No ○ N/A ○ No Response ○

Number	Family	Basic/Derived
3.1.1	ACCESS CONTROL	Basic

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

SUGGESTED EVIDENCE: Access Control Policy, copy of group access structure, priviliged 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:

Comment:

Attachments

Comply	Partial	No	N/A	No Response
0	0	0	0	109

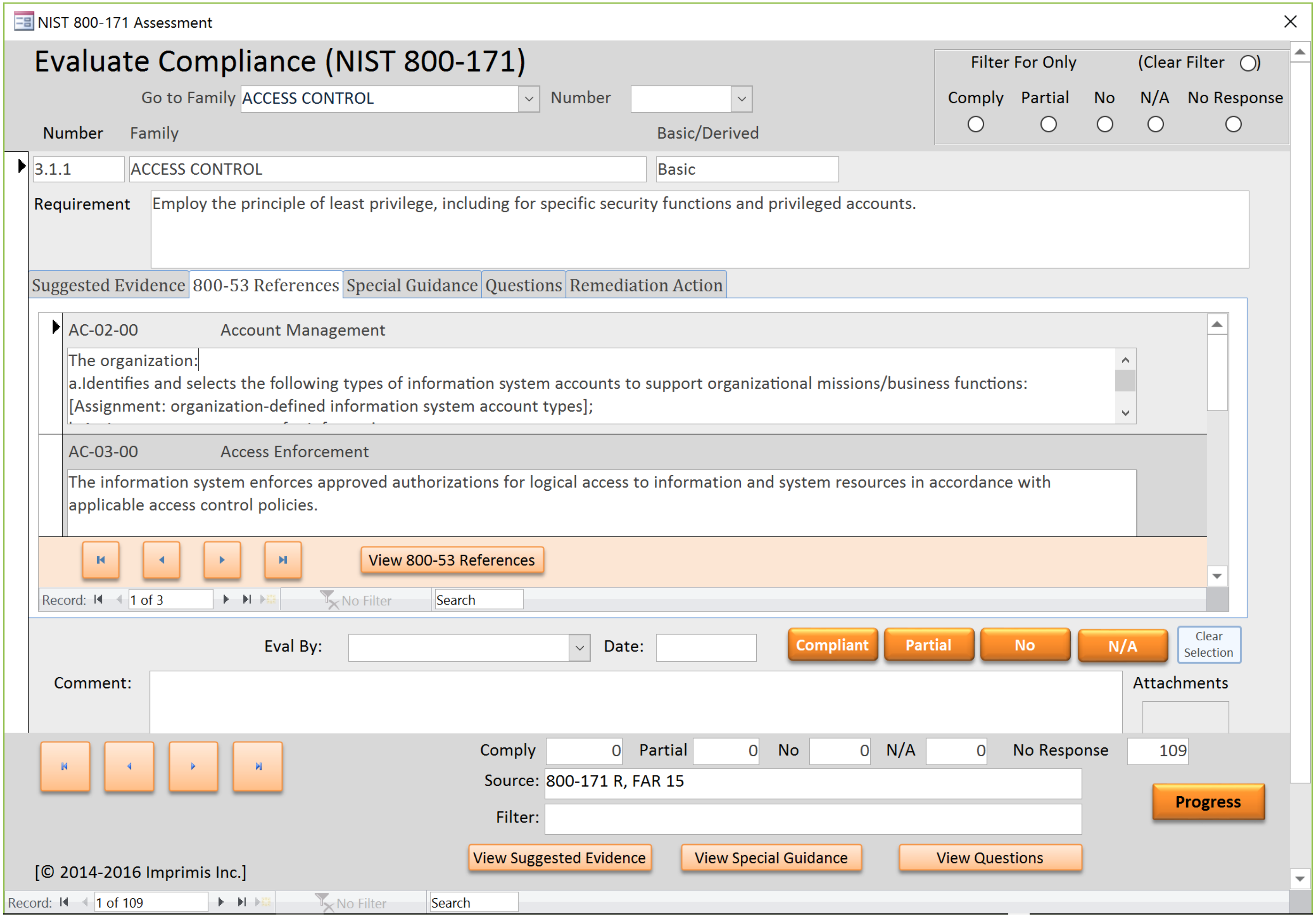
Source: 800-171 R, FAR 15

Filter:

[© 2014-2016 Imprimis Inc.]

Record: 1 of 109 No Filter Search

Self Assessment – 800-53 Reference



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family: ACCESS CONTROL Number:

Filter For Only (Clear Filter ○)
Comply ○ Partial ○ No ○ N/A ○ No Response ○

Number	Family	Basic/Derived
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 | Questions | Remediation Action

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:

Comment:

Attachments

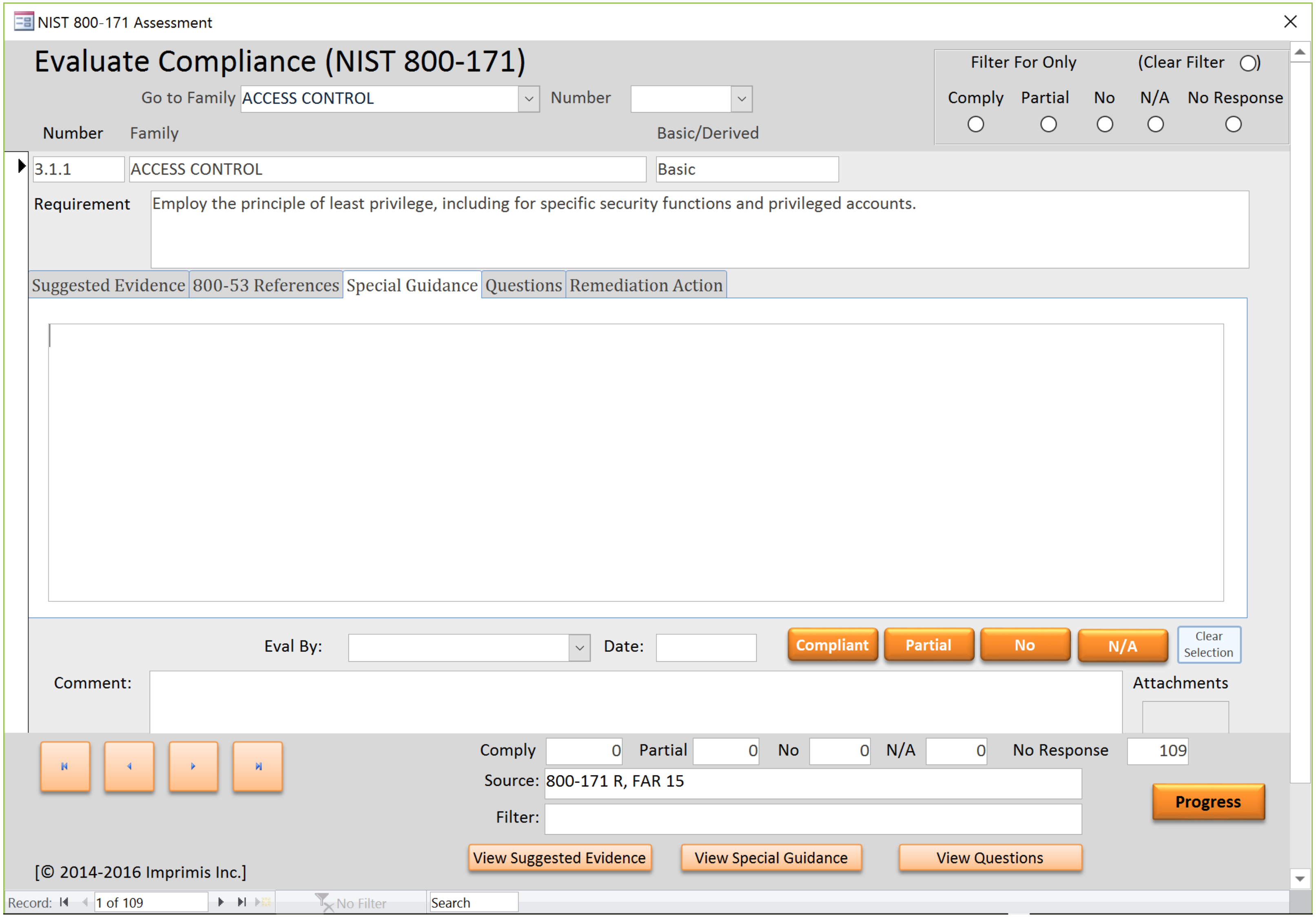
Comply	0	Partial	0	No	0	N/A	0	No Response	109

Source: 800-171 R, FAR 15

Filter:

[© 2014-2016 Imprimis Inc.]

Self Assessment - Guidance



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family: ACCESS CONTROL
Number:

Filter For Only (Clear Filter ○)
Comply ○ Partial ○ No ○ N/A ○ No Response ○

Number	Family	Basic/Derived
3.1.1	ACCESS CONTROL	Basic

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

Eval By:
Date:

Comment:

Attachments

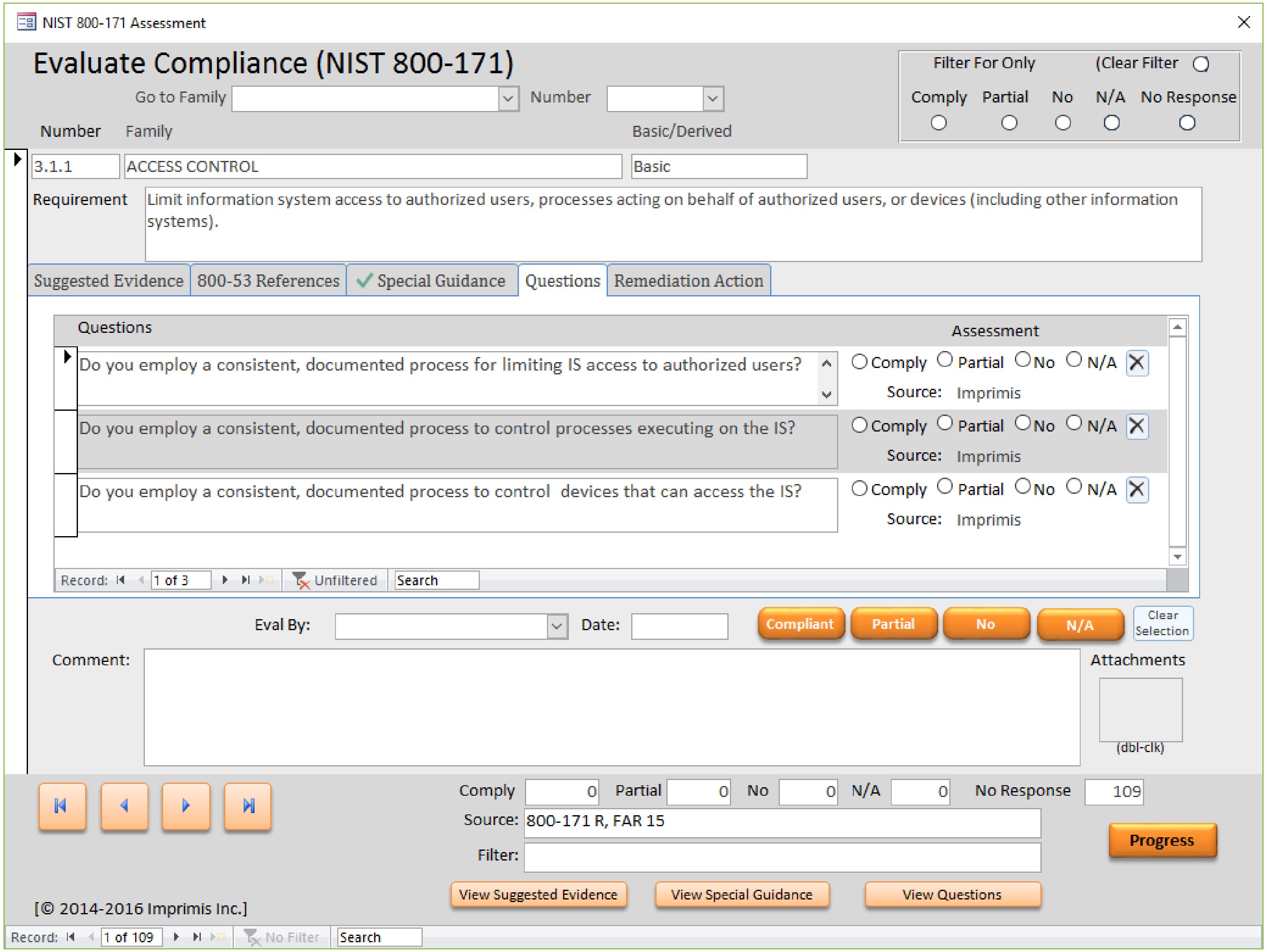
Comply	0	Partial	0	No	0	N/A	0	No Response	109

Source: 800-171 R, FAR 15
Filter:

[© 2014-2016 Imprimis Inc.]

Record: 1 of 109 No Filter Search

Self Assessment - Questions



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family: 　 Number:

Filter For Only (Clear Filter ○

Comply	Partial	No	N/A	No Response
○	○	○	○	○

Number	Family	Basic/Derived
3.1.1	ACCESS CONTROL	Basic

Requirement: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Suggested Evidence | 800-53 References | ✓ Special Guidance | Questions | Remediation Action

Questions	Assessment
Do you employ a consistent, documented process for limiting IS access to authorized users?	○ Comply ○ Partial ○ No ○ N/A ☒ Source: Imprimis
Do you employ a consistent, documented process to control processes executing on the IS?	○ Comply ○ Partial ○ No ○ N/A ☒ Source: Imprimis
Do you employ a consistent, documented process to control devices that can access the IS?	○ Comply ○ Partial ○ No ○ N/A ☒ Source: Imprimis

Record: 1 of 3 　 Unfiltered 　 Search

Eval By: 　 Date:

Comment:

Attachments
(dbl-clk)

Comply	Partial	No	N/A	No Response
0	0	0	0	109

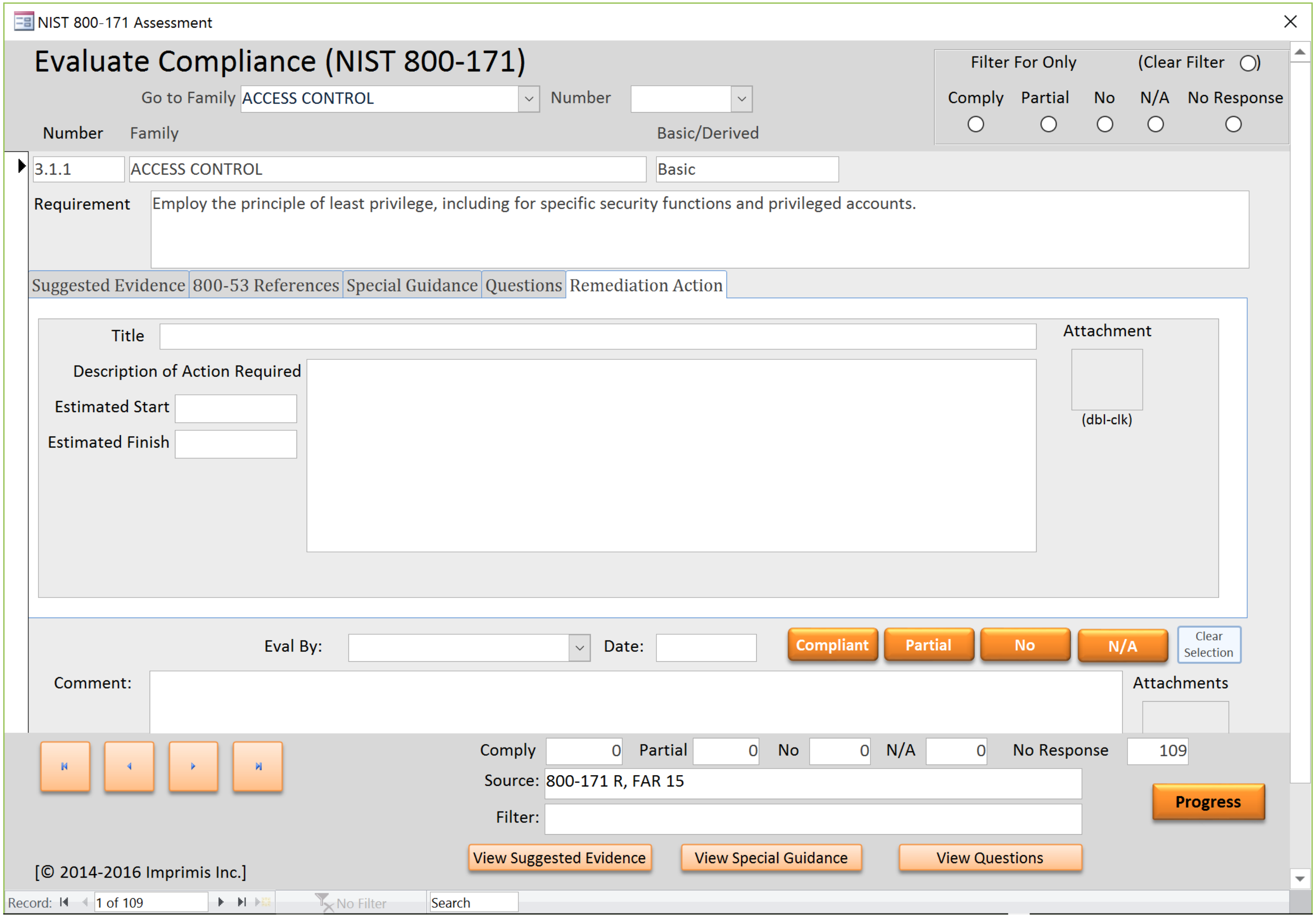
Source: 800-171 R, FAR 15

Filter:

Record: 1 of 109 　 No Filter 　 Search

Self Assessment - Remediation

Proud to be 100% Employee Owned



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family: ACCESS CONTROL

Number:

Filter For Only (Clear Filter ○)

Comply ○ Partial ○ No ○ N/A ○ No Response ○

Number	Family	Basic/Derived
3.1.1	ACCESS CONTROL	Basic

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

Title:

Description of Action Required:

Estimated Start:

Estimated Finish:

Attachment (dbl-clk)

Eval By:

Date:

Comment:

Attachments

Comply: 0 Partial: 0 No: 0 N/A: 0 No Response: 109

Source: 800-171 R, FAR 15

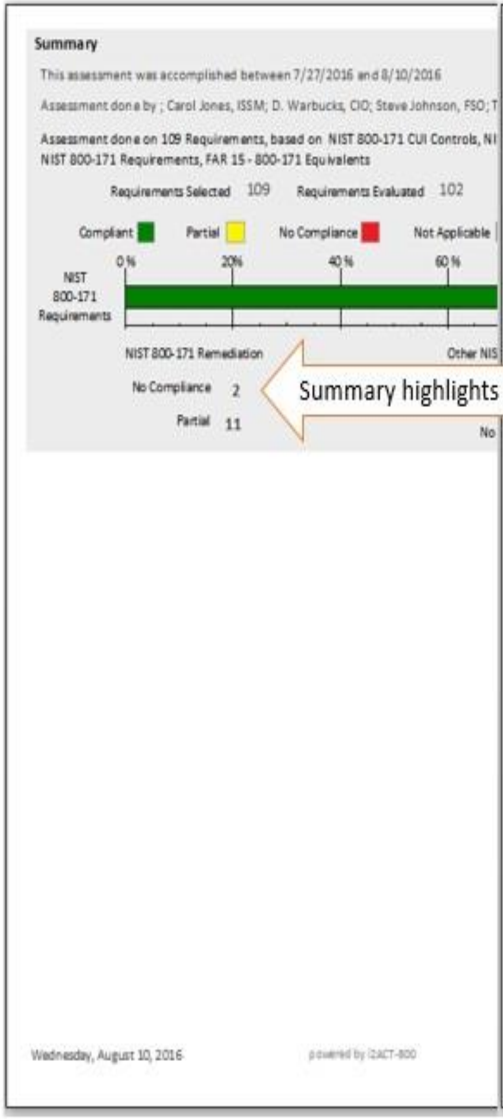
Filter:

[© 2014-2016 Imprimis Inc.]

Record: 1 of 109

Self Assessment - Remediation Report

Proud to be 100% Employee Owned



Summary

This assessment was accomplished between 7/27/2016 and 8/10/2016

Assessment done by ; Carol Jones, ISSM; D. Warbucks, CIO; Steve Johnson, FSO; T

Assessment done on 109 Requirements, based on NIST 800-171 CUI Controls, NI
NIST 800-171 Requirements, FAR 15 - 800-171 Equivalents

Requirements Selected 109 Requirements Evaluated 102

NIST 800-171 Remediation

No Compliance	2
Partial	11

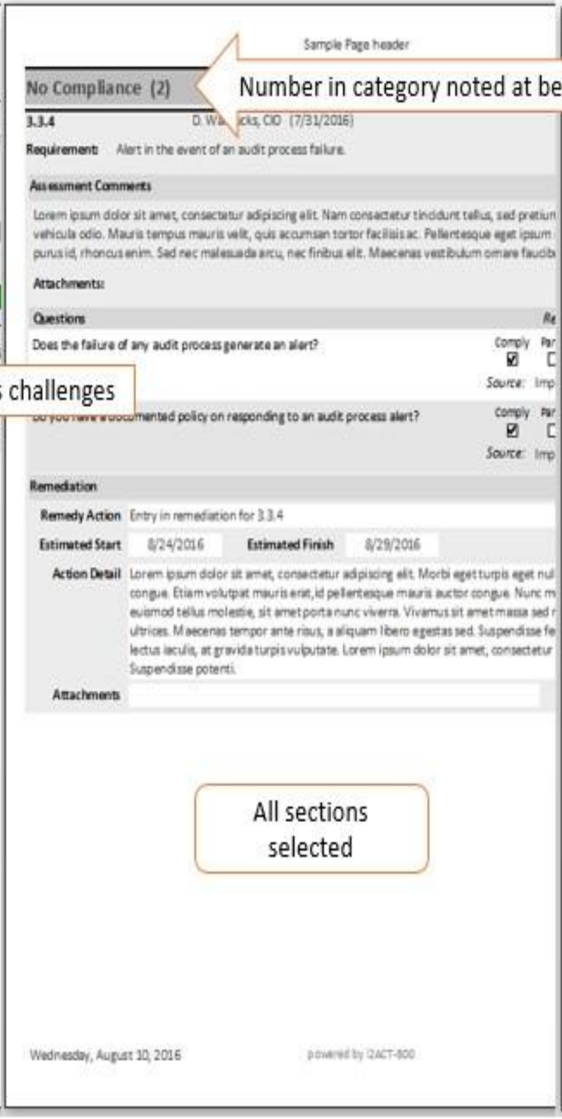
Other NIS

No

Wednesday, August 10, 2016

powered by i2ACT-800

Summary highlights challenges



Sample Page header

No Compliance (2)

3.3.4 D. Warbucks, CIO (7/31/2016)

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

Assessment Comments

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam consectetur tincidunt tellus, sed pretium vehicula odio. Mauris tempus mauris velit, quis accumsan tortor facilisis ac. Pellentesque eget ipsum purus id, rhoncus enim. Sed nec malesuada arcu, nec finibus elit. Maecenas vestibulum ornare faucib

Attachments:

Questions Re

Does the failure of any audit process generate an alert? Comply ☑ Par ☐ Source: Imp

Do you have a documented policy on responding to an audit process alert? Comply ☑ Par ☐ Source: Imp

Remediation

Remedy Action Entry in remediation for 3.3.4

Estimated Start 8/24/2016 **Estimated Finish** 8/29/2016

Action Detail Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi eget turpis eget nul congue. Etiam volutpat mauris erat, id pellentesque mauris auctor congue. Nunc m euismod tellus molestie, sit amet porta nunc viverra. Vivamus sit amet massa sed r ultrices. Maecenas tempor ante risus, a aliquam libero egestas sed. Suspendisse fe lectus iaculis, at gravida turpis vulputate. Lorem ipsum dolor sit amet, consectetur Suspendisse potenti.

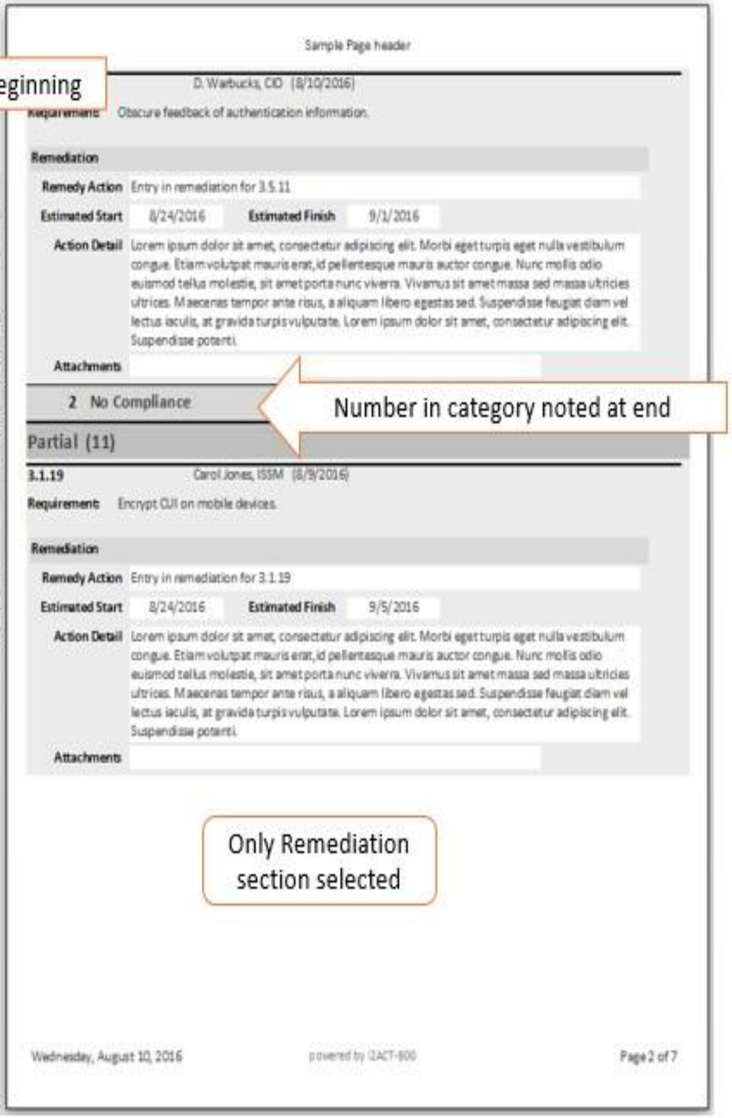
Attachments

Wednesday, August 10, 2016

powered by i2ACT-800

Number in category noted at beginning

All sections selected



Sample Page header

D. Warbucks, CIO (8/10/2016)

Requirement: Obscure feedback of authentication information.

Remediation

Remedy Action Entry in remediation for 3.5.11

Estimated Start 8/24/2016 **Estimated Finish** 9/1/2016

Action Detail Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi eget turpis eget nulla vestibulum congue. Etiam volutpat mauris erat, id pellentesque mauris auctor congue. Nunc mollis odio euismod tellus molestie, sit amet porta nunc viverra. Vivamus sit amet massa sed massa ultricies ultrices. Maecenas tempor ante risus, a aliquam libero egestas sed. Suspendisse feugiat diam vel lectus iaculis, at gravida turpis vulputate. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse potenti.

Attachments

2 No Compliance

Partial (11)

3.1.19 Carol Jones, ISSM (8/9/2016)

Requirement: Encrypt CUI on mobile devices.

Remediation

Remedy Action Entry in remediation for 3.1.19

Estimated Start 8/24/2016 **Estimated Finish** 9/5/2016

Action Detail Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi eget turpis eget nulla vestibulum congue. Etiam volutpat mauris erat, id pellentesque mauris auctor congue. Nunc mollis odio euismod tellus molestie, sit amet porta nunc viverra. Vivamus sit amet massa sed massa ultricies ultrices. Maecenas tempor ante risus, a aliquam libero egestas sed. Suspendisse feugiat diam vel lectus iaculis, at gravida turpis vulputate. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse potenti.

Attachments

Wednesday, August 10, 2016

powered by i2ACT-800

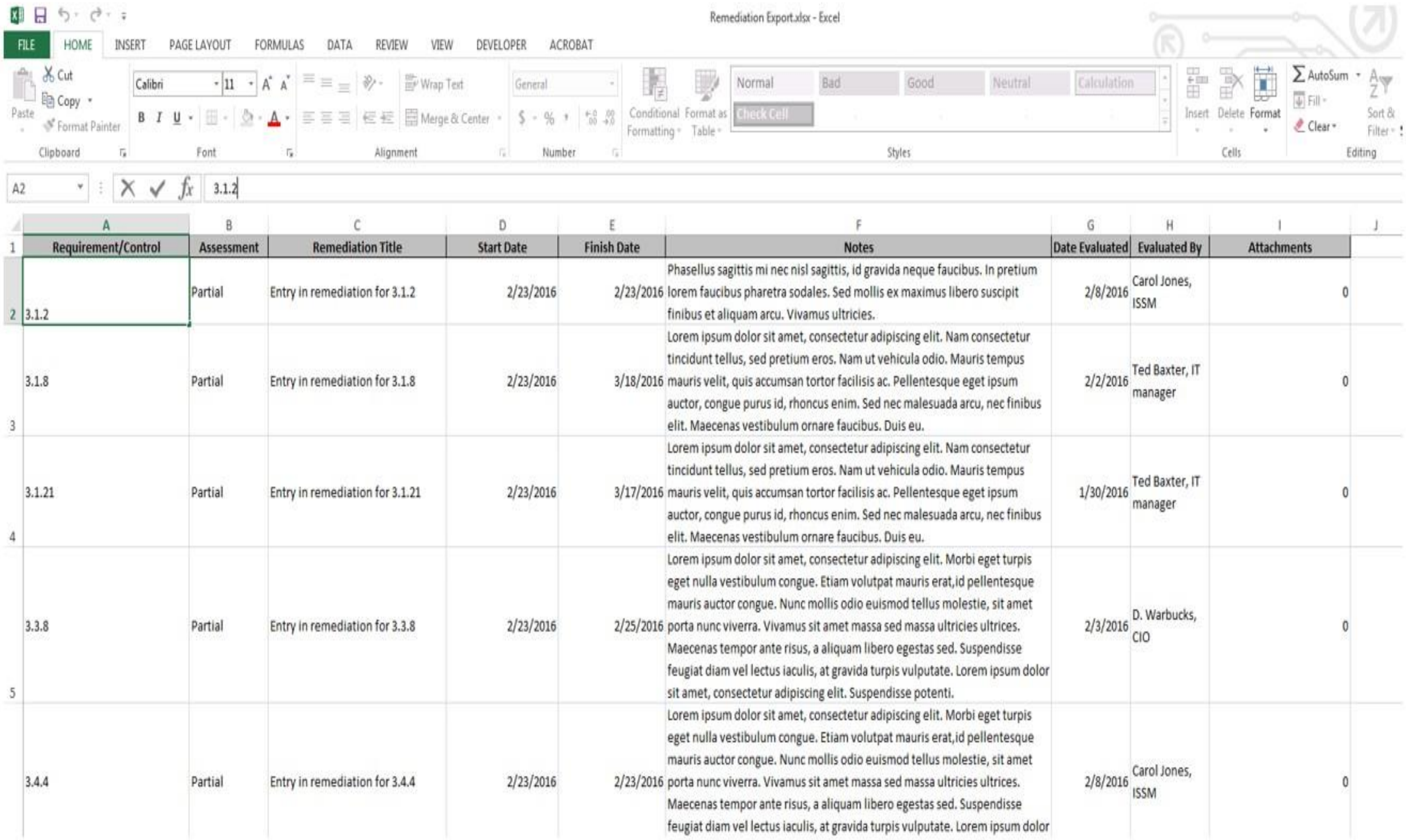
Page 2 of 7

Number in category noted at end

Only Remediation section selected

Self Assessment - POAM

Proud to be 100% Employee Owned



Remediation Export.xlsx - Excel

3.1.2

	A	B	C	D	E	F	G	H	I
1	Requirement/Control	Assessment	Remediation Title	Start Date	Finish Date	Notes	Date Evaluated	Evaluated By	Attachments
2	3.1.2	Partial	Entry in remediation for 3.1.2	2/23/2016	2/23/2016	Phasellus sagittis mi nec nisl sagittis, id gravida neque faucibus. In pretium lorem faucibus pharetra sodales. Sed mollis ex maximus libero suscipit finibus et aliquam arcu. Vivamus ultricies.	2/8/2016	Carol Jones, ISSM	0
3	3.1.8	Partial	Entry in remediation for 3.1.8	2/23/2016	3/18/2016	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam consectetur tincidunt tellus, sed pretium eros. Nam ut vehicula odio. Mauris tempus mauris velit, quis accumsan tortor facilisis ac. Pellentesque eget ipsum auctor, congue purus id, rhoncus enim. Sed nec malesuada arcu, nec finibus elit. Maecenas vestibulum ornare faucibus. Duis eu.	2/2/2016	Ted Baxter, IT manager	0
4	3.1.21	Partial	Entry in remediation for 3.1.21	2/23/2016	3/17/2016	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam consectetur tincidunt tellus, sed pretium eros. Nam ut vehicula odio. Mauris tempus mauris velit, quis accumsan tortor facilisis ac. Pellentesque eget ipsum auctor, congue purus id, rhoncus enim. Sed nec malesuada arcu, nec finibus elit. Maecenas vestibulum ornare faucibus. Duis eu.	1/30/2016	Ted Baxter, IT manager	0
5	3.3.8	Partial	Entry in remediation for 3.3.8	2/23/2016	2/25/2016	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi eget turpis eget nulla vestibulum congue. Etiam volutpat mauris erat,id pellentesque mauris auctor congue. Nunc mollis odio euismod tellus molestie, sit amet porta nunc viverra. Vivamus sit amet massa sed massa ultricies ultrices. Maecenas tempor ante risus, a aliquam libero egestas sed. Suspendisse feugiat diam vel lectus iaculis, at gravida turpis vulputate. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse potenti.	2/3/2016	D. Warbucks, CIO	0
	3.4.4	Partial	Entry in remediation for 3.4.4	2/23/2016	2/23/2016	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi eget turpis eget nulla vestibulum congue. Etiam volutpat mauris erat,id pellentesque mauris auctor congue. Nunc mollis odio euismod tellus molestie, sit amet porta nunc viverra. Vivamus sit amet massa sed massa ultricies ultrices. Maecenas tempor ante risus, a aliquam libero egestas sed. Suspendisse feugiat diam vel lectus iaculis, at gravida turpis vulputate. Lorem ipsum dolor	2/8/2016	Carol Jones, ISSM	0

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?