Quick Start Strategy to Compliance
DFARS 252.204-7012

Rob Gillen
Overview

• Meet Bill Harrison
• Meet FASTLANE
• Important Updates
• Overview of NIST 800-171
• Case Studies
• **5 Items to a Quick Start Strategy to Compliance...NIST 800-171/DFARS**
  1. Boundary Definition
  2. Cybersecurity Policies
  3. Technical Assessment
  4. System Security Plan (SSP) and Plan of Actions and Milestones (POA&M)
  5. Continuous Monitoring
Important Updates

• NIST 800-171 Rev 1 Update Released 28 Nov 2017
• NIST 800-171A in draft
  – Assessment guide
  – Provides testing (assessment) guidance
  – Requesting industry feedback – comments due 27 Dec 2017
  – Derived from NIST 800-53A
  – Assist organizations in:
    • Developing assessment plans
    • Conducting assessments
What is NIST 800-171?

- Protection of Controlled Unclassified Information (CUI) in non-federal systems
- Executive Order 13556 – National Archives and Record Administration (NARA) as executive agent
- DoD, GSA and NASA require contractors to implement specific security measures and report non-compliance to the CIO by December 2017
- What's covered??
  - Anything related to "performance of the contract"
CUI Categories Defined by NARA

- Agriculture
- Controlled Technical Information
- Critical Infrastructure
- Emergency Management
- Export Control
- Financial
- Geodetic Product Information
- Immigration
- Information Systems Vulnerability Information
- Intelligence
- International Agreements
- Law Enforcement
- NATO Information
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business
- SAFETY Act Information
- Statistical
- Tax
- Transportation
NIST 800-171 Security Families

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance

- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity
5 ITEMS TO A QUICK START STRATEGY TO COMPLIANCE...NIST 800-171/DFARS
• Where does my CUI reside?
• Minimize the CUI footprint within your organization
• Define what systems, processes, programs, applications, hardware, software, people, etc. fall under the scope of your NIST 800-171 compliance
• Understand dataflow to know:
  – What users and components have direct access to CUI?
  – What users and components have indirect access to CUI?
  – What users and component control access to CUI?
Simple Boundary

- Understand which IT assets fit within the boundary.
- Interconnections: indicate and label interconnections to other systems.
- Make sure your boundary is consistent with hardware & software inventory.
- Make sure your diagrams are consistent with boundary descriptions.
Large majority of the CUI controls in 800-171 are policy based.
Starting with strong organizational policies will enforce process and compliance.
Supplementing current policies with new requirements provides less impact.
Phase in new policies.
Determine to whom and what the new policies apply.
Educate all staff on new policies.
Any policies requiring new technology, processes or personnel must be analyzed within the organizational strategy.
#3 Technical Assessment

- Assess your current security status IAW NIST 800-171
- Conduct a gap analysis to determine non-compliance
- FIPS 140-2 encryption for CUI?
- Data-at-Rest solution?
- Multi-factor authentication?
- Audit logging, review and management?
- Incident Response?
• System Security Plan (SSP) identifies compliance with NIST 800-171 security controls
• 14 families of security controls
• Focused around confidentiality
• Based on FIPS 200
• Ensure compliance with any deficiencies identified in your gap analysis or request approval from CIO.
• Plan of Actions and Milestones (POA&M) is developed
#5 Continuous Monitoring

- Compliance is a full-time commitment
- Not just documentation
- Can be implement in cloud-based solutions or on premise
- Requires a policy, procedures and tools to implement
- Automation is KEY!
Boundary Definition
Know what is included in your CUI boundary.

Policy and Personnel
Policy drives compliance and procedures for meeting the technical requirements.

Technical Assessment
Review all technical controls in place against the NIST 800-171 requirements

System Security Plan
The backbone to your system documentation.

Continuous Monitoring
Full-time commitment.
Nothing in this presentation is an endorsement of a particular company, technology or solution!

Names and titles of the guilty parties have been changed!
15 People IT contracting company providing out-sourcing solutions, such as website hosting, IT maintenance and network management to prime contractors. Mostly remote employees.

Gap Analysis Findings

• No Data at Rest (DAR) solutions
• No Multi-Factor Authentication (MFA)
• No organizational policies documented.
• No background checks conducted on employees.
• No vulnerability assessments conducted on internal assets.
• No configuration management of internal assets.
• .....................

Solutions to Compliance

• Deployed FIPS-compliant BitLocker for Windows 10 laptops.
• Legacy laptops were upgraded.
• YubiKey for local authentication to Windows laptops
• POA&M documented and employee handbook drafted.
• Employee handbook updated to ensure that all employees hired who worked on DoD prime contractor sites have background checks conducted
• POA&M documented and Vulnerability management policy drafted. All users will be required to bring their laptop in monthly for scanning.
• POA&M documented and a CM Program initiated. Initial policy developed and asset inventory completed.
• Many more POA&M items developed and incorporated into a Cybersecurity Strategy that requires executive buy-in
Case Study #2: Carillon Defense Contractor

50 employee company providing mostly sub-contractor support to DoD contracts. Most work is conducted at government site. Some work is completed at contractor site.

**Gap Analysis Findings**

- DAR is deployed on laptops using BitLocker, but not in FIPS mode
- No MFA – using Active Directory
- No centralized auditing solution
- No incident response program

**Solutions to Compliance**

- Reconfigure laptops with FIPS-compliant BitLocker
- Implement Azure Multi-Factor Authentication Server to work with AD FS in Windows Server
- POA&M documented and centralized auditing solution TBD
- POA&M documented, incident response policy drafted and working to contract a MSSP
350 employees. Most sit on contractor site. Full network configured on premise. Manufacture parts for DoD equipment.

**Gap Analysis Findings**
- No continuous monitoring strategy
- No incident response program
- No centralized auditing solution

**Solutions to Compliance**
- POA&M documented and working to deploy Nessus Security Center
- POA&M documented, incident response policy drafted and working to contract a MSSP
- POA&M documented and centralized auditing solution TBD
SOLUTIONS PROVIDERS
Secure Cyber Defense, LLC

Shawn Walker
Chief Technical Officer
Secure Cyber Defense
Shawn.walker@securecyberdefense.com
(937) 751-4047
Who are we?

- Founded Jan 1 2015
- Founders former Law Enforcement and Military
- Dedicated to the small to mid-market
- Affordable entry to advanced Cybersecurity solutions
- Current customers include financial, legal, manufacturing, real estate, health care, local gov’t and DoD contractor.
Does this apply to me?

1. Every contract and solicitation will include DFARS 252.204-7012
3. Can I scope this?

If so, what do I need to do by December 31, 2017?

1. System Security Plan - How the security controls in NIST 800-171r1 are implemented, and a network map including boundaries and interconnections.
2. Plan of Action - For the controls that are not implemented, what is the plan for compliance and when will it be implemented?
What can I do?

- Become familiar with the requirement
  - DFARS 252.204-7012
  - NIST SP 800-171r1

- Cyber Security Enhancement Tool (CSET)
  https://www.us-cert.gov/forms/csetiso

- NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171
What does SCD offer?

Secure Cyber Defense Compliance and Planning Engine (CAPE)

- Includes resources to achieve compliance
  - Incident Response Template
  - Maintenance Log
  - Media Control Log
  - Mobile Device Acceptable Use Policy
  - Risk Assessment
  - Visitor Log

- Each control is explained in plain language with selectable recommendation for each on how to achieve compliance

- Produces System Security Plan and POAM needed for 31 Dec 2017 deadline

- Expert security review within 24 hours of completion by our staff

- Only $995!!! $15K value!!!

- www.securecyberdefense.com/cape
What does SCD offer?

**On-site/Remote assessment**

- Includes an in-person or remote assessment of the organization's compliance to NIST 800-171 as well as a vulnerability scan.
- DFARS Cyber Roadmap that includes the assessed results and custom recommendations for each that are out of compliance.
- The customer receives:
  - System Security Plan
  - Plan of Action and Milestones
  - Results of the vulnerability scan
  - Customized services should you choose to outsource
- Priced based on size and number of locations - Contact us today!
  info@securecyberdefense.com
What does SCD offer?

**Consulting hours**

- For the customer who is working through their assessment and wants some guidance and clarification
- Email us for pricing - info@securecyberdefense.com
Our Service Offerings

- Vulnerability Scanning
- Cybersecurity Roadmap
- Managed Security Services
- Cybersecurity Consulting
- Cyber Policy
- Staff Training
- SIEM
- Forensic Logging
Questions?

www.securecyberdefense.com
time is money

Cyber security economics analyzes the resources and time spent by the bad guys to break into a system versus resources and time spent by the good guys to protect, maintain, and recover. Relative time and/or effort is a fundamental metric.

where are you spending yours?

Cybereconomics

Rebecca Onuskanich, CISSP
Cybernetic Security Engineer
972.955.2348 / becca@tenet3.com
Tenet3 Overview

• A computer science / engineering firm
  – Full “stack” software/hardware capabilities
  – Visualizing “Big Cyber”
  – Providing strategic analysis

• We develop metrics to assess
  – Threat mitigation strategies
  – Security costs
    • Defender vs. Adversary costs
  – Residual risks and resiliency

• Breach prevention, response, recovery
  – Prevention is optional
  – Response is not optional
  – Given a choice, go with prevention
Security Strategy Begins with Taking Stock

• Inventory your stuff
  – Enumeration

• Organize it Across Layers
  – Aggregation

• Show how various system views are connected
  – Abstraction

Count
Collect
Connect
Know Your Vulnerabilities – Stay Informed

- Your vulnerabilities are defined by the intersection of
  - Your system’s susceptibility (weaknesses)
  - An attacker’s access (your system’s exposure)
  - An attacker’s capability

- These can change over time!
  - Your updates can alter susceptibilities (add or drop)
  - Attacker access can grow (new employees, new attackers, new exposure)
  - Attacker capabilities usually grow over time

- Tomorrow’s risks will almost certainly be worse
  - Even good risk assessments have a limited shelf life and can rapidly grow stale
Applying NIST 800-171 controls around your CUI boundary reduces the 3 Tenets of a possible attack or breach of data.

1. System Susceptibility
   - Configuration Management
   - User Awareness Training
   - Continuous Monitoring
   - Software Assurance

2. Threat Accessibility
   - Access Control
   - Cryptography
   - Security Engineering
   - Remote Access
   - Physical Control

3. Threat Capability
   - Penetration Testing
   - Insider Threat
   - Resiliency
   - Boundary Defenses
   - STIX, etc

Successful Attack Possible
CONTINUOUS MONITORING

The key to success is continuous monitoring of the NIST 800-171 CUI program. Our team will work with you to develop an actionable plan to maintain compliance.

IMPLEMENTATION PLAN

After the conclusion of the Assessment Phase, our team will execute the Roadmap provided at the completion of the Assessment Phase. This Implementation Phase will include awareness and training for your staff.

ASSESSMENT

In this phase our team of certified experts will conduct a complete Gap Assessment of your organization, system and program against the NIST 800-171 requirements. Your organization will be provided with a complete Roadmap to compliance.

ECONOMICS DRIVEN

Our solutions are based around our proprietary algorithms of defender/adversary work-factor costs allowing executive management to make cybersecurity financial decisions based on statistical facts.

INTRODUCTION

Compliance processes are reliant on relationships and education. Our team will educate your staff on the NIST 800-171 requirements, along with the expectations for the upcoming Assessment and Implementation Phases.
Cybersecurity Strategy
- Management Initiative for Cybersecurity and Compliance.

Updated Policies
- Handbook updates to reflect cybersecurity strategy
- Development and implementation of new cybersecurity policies

Awareness Training Program
- Train all users in cybersecurity training
- Require initial and annual refresher training

Procedures
- Development and enforcement of cybersecurity procedures

Continuous Monitoring Strategy
- Develop and implement a continuous monitoring strategy to support continuous improvement and compliance
- POA&M remediation actions
Questions?

Rebecca Onuskanich, CISSP
becca@tenet3.com
Why use the Cloud for DFARS Compliance?

DFARS Compliance via DoD Approved Cloud

Use Cloud to work with Customer(s) and Subs

Get operational in 10 days
3 Actions for Cloud DFARS Compliance to get started by Dec 31/17

• Action #1: Use a DoD Approved Cloud

• Action #2: Notify Contracting Officer per DFARS

• Action #3: POAM for your network, devices and people
Action #1: DoD Approved Cloud For DFARS Compliance

Action: Use FedRAMP site to confirm DoD Approved Cloud

FedRAMP Moderate is required for CUI documents storage, collaboration and transmission done at DoD Approved Cloud

Suggested: Use this link to review FedRAMP offerings
https://www.fedramp.gov/
Action #2: Cloud DFARS Compliance Notice to my Contracting Officer

Action : Use a DoD Approved Cloud with SaaS and send notice to CO

CO Notice Required:
DFARs 252.239-7010 Cloud Computing Services
Action #3: Set up cloud site
And your network that is DFARS Compliant

Action: Subscribe to a DoD Approved Cloud that has Software as a Service (SaaS) to Store, Work on and Transmit CUI

Suggested: Use DFARs Compliant DoD Approved Cloud and Secure Your Network i.e. Encrypt Devices

Key Point: use DoD Approved Cloud SaaS also used by DoD
Why the Cloud for DFARS Compliance?

DOD Approved Cloud

Encrypt all CUI for sending to Secure Cloud

Network Components

Boundary Protection

Port Protocols and Services

Outside the System Boundary

Different System Outside the Boundary

Interconnections

System Boundary

Network Architecture
Why use Cloud for DFARS Compliance?

• Savings: Steps #1, 2 and #3 concurrently - in 10 days!

• Uses 80/20 Rule:
  – 80% documents/collaborations/transmission on DoD Approved Cloud
  – Focus 20% of your effort on your own security and policy

• Immediate Security at DoD Cloud: Over 200 NIST controls

Use what DoD has approved.
What’s Next

• Do Steps #1, #2 and #3 to get started

• Set up a trial deployment

• Get DFARS Compliant at a DoD Approved Cloud!
Afternoon Session

Quick Start Strategy to Compliance
DFARS 252.204-7012
Secure Cyber Defense, LLC

Shawn Walker
Chief Technical Officer
Secure Cyber Defense
Shawn.walker@securecyberdefense.com
(937) 751-4047
Who are we?

- Founded Jan 1 2015
- Founders former Law Enforcement and Military
- Dedicated to the small to mid-market
- Affordable entry to advanced Cybersecurity solutions
- Current customers include financial, legal, manufacturing, real estate, health care, local gov’t and DoD contractor.
CYBER SECURITY
FOR YOUR BUSINESS

Your organization will be hacked, what you do right now will determine if you and your organization end up in the headlines and on the wrong side of a press release.

I WANT MY ORGANIZATION SECURE

CONTACT US FOR A FREE, NO OBLIGATION CONSULTATION

Statistics Don't Matter
Unless You Are One Of Them.

We provide security assessments, risk analysis, consulting, training, IT staff augmentation and threat monitoring to small and mid-sized organizations.
To access this content, you must purchase NIST 800-171 Compliance and Planning Engine Access, or log in if you are a member.

CAPE Makes Compliance Easy

To support your organization with Controlled Unclassified Information (CUI) compliance registration, we offer this custom tool, called the Secure Cyber Defense Compliance and Planning Engine, or CAPE.

CAPE provides resources to assist in achieving compliance, including an incident response template, a maintenance log, a media control log, mobile device acceptable use policy, risk assessment, visitor log, and security assessment. When complete, you will have a System Security Plan and Plan of Action, which are the two critical documents required by December 31, 2017.
NIST 800-171 Compliance and Planning Engine

CAPE Downloadable Instructions

NOTE: CAPE has been improved! The “Next” button will now save your progress! Save and Exit is no longer needed and has been removed.

PROCEED TO FORM
My Account

- Documents
- Compliance Engine Instructions
- Return to Compliance Form
- Orders
- Subscriptions
- Account details
- Logout
Documents

Incident Response Plan
Maintenance Log
Media Control Log
Mobile Device Acceptable Use Policy
Risk Assessment
Visitor Log
Primary POC *
Shawn Walker

Email *
shawn.walker@secdefllc.com

Phone *
(937) 353-7504

Main company location *
31 South Second St

Street Address
Suite 202

Address Line 2
Miamisburg

City
45342

State / Province / Region
OH

Country
United States

# of physical locations *
1

Please enter a value greater than or equal to 2.
NIST 800-171 Compliance And Planning Engine

CAPE

3.1 ACCESS CONTROL    3.2 AWARENESS AND TRAINING    3.3 AUDIT AND ACCOUNTABILITY
3.4 CONFIGURATION MANAGEMENT    3.5 IDENTIFICATION AND AUTHENTICATION    3.6 INCIDENT RESPONSE
3.7 MAINTENANCE    3.8 MEDIA PROTECTION    3.9 PERSONNEL SECURITY    3.10 PHYSICAL PROTECTION
3.11 RISK ASSESSMENT    3.12 SECURITY ASSESSMENT    3.13 SYSTEM AND COMMUNICATIONS PROTECTION
3.14 SYSTEM AND INFORMATION INTEGRITY
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems).

- Yes
- No
- N/A or Alternative Security Measure

Every user that accesses a Company system must have a user account assigned to them from an administrator. The only access permitted to the information system must include at least a username and password.

Explain how this control is met

Only users with valid user accounts and passwords are permitted access to the information system.
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Yes

No

N/A or Alternative Security Measure

If your organization develops software, security principles must be applied at various levels of development. This control also covers employing solid principles in the design of the network. For example, a firewall with a network switch and a domain used to administer the network and enforce security controls is a good foundation for most networks.

If you believe this control is not applicable or that an alternative security measure is equally effective you must describe it here. When you notify Contracting that you have N/As or alternative security controls they will send it to the DoD CIO for review and approval.

No collaborative devices are in use at this facility.
3.3.3 Review and update audited events.

- Yes
- No
- N/A or Alternative Security Measure

Do you review your auditing policy periodically?

Plan for compliance

- (Recommendation) Audit policy must include requirement for reviewing audited events periodically and updating as needed. 'Annually, the audit policy will be reviewed and updated as needed'
- SCD - Managed Auditing
- Other

Date of implementation

[Input field]

[Next] [Previous] [Skip question for now] [Skip to last page]
3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

No

Plan for compliance

(Recommendation) Implement threat management, indicators of compromise, intrusion detection system, or an intrusion prevention system either on the firewall or a separate device. Once implemented, the tools will be monitored for potential attacks.

Date of implementation

08/18/2018

3.14.7 Identify unauthorized use of the information system.

No

Plan for compliance

SCD - Firewall as a Service and Security Delivery Service

Date of implementation

Confirmation
# System Security Plan

Secure Cyber Defense will contact you within 24 hours for a scoping call based on the services you selected. At that time you will also receive a quote for services. Direct any questions to cuihelp@securecyberdefense.com. Thank you!

<table>
<thead>
<tr>
<th>Plan of Action</th>
<th>System Security Plan</th>
<th>Alternate Security Measures</th>
<th>All</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>NIST 800-171 Control</th>
<th>Compliant</th>
<th>Plan for compliance</th>
<th>Estimated implementation date</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.</td>
<td>No</td>
<td>I like collusions we’re keeping this.</td>
<td>2017-10-27</td>
</tr>
</tbody>
</table>
at appropriate locations within organizational information systems.

<table>
<thead>
<tr>
<th>3.14.3 Monitor information system security alerts and advisories and take action in response.</th>
<th>No</th>
<th>(Recommendation) Sign up for alerts at <a href="https://www.us-cert.gov/ncas/alerts">https://www.us-cert.gov/ncas/alerts</a> Implement procedures to verify systems are protected against new threats. Document in a written policy.</th>
<th>2018-01-19</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.14.4 Update malicious code protection mechanisms when new releases are available.</td>
<td>Yes</td>
<td>Completed.</td>
<td></td>
</tr>
<tr>
<td>3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.</td>
<td>Yes</td>
<td>Completed.</td>
<td></td>
</tr>
<tr>
<td>3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.</td>
<td>Yes</td>
<td>Completed.</td>
<td></td>
</tr>
<tr>
<td>3.14.7 Identify unauthorized use of the information system.</td>
<td>Yes</td>
<td>Completed.</td>
<td></td>
</tr>
<tr>
<td>NIST 800-171 Control</td>
<td>Compliant</td>
<td>Plan for compliance</td>
<td>Method of compliance</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).</td>
<td>No</td>
<td>(Recommendation) Document and implement, ‘Only users with approved user accounts are authorized access to the’</td>
<td></td>
</tr>
<tr>
<td>3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.</td>
<td>No</td>
<td>(Recommendation) Create Security groups in Active Directory and assign those groups to applicable folders. Lock down</td>
<td></td>
</tr>
<tr>
<td>3.1.3 Control the flow of CUI in accordance with approved authorizations.</td>
<td>No</td>
<td>(Recommendation) Document the following policy: ‘All CUI transmitted via email is encrypted and only sent to</td>
<td>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
</tr>
<tr>
<td>3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.</td>
<td>Yes</td>
<td></td>
<td>Personnle designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
</tr>
<tr>
<td>3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts</td>
<td>No</td>
<td>(Recommendation) Admin account access will be limited to privileged users who will be identified in writing.</td>
<td>Only non-admin accounts are permitted to logon to perform everyday nonsecurity related activities. The use of admin</td>
</tr>
<tr>
<td>3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.</td>
<td>Yes</td>
<td></td>
<td>Only non-admin accounts are permitted to logon to perform everyday nonsecurity related activities. The use of admin</td>
</tr>
<tr>
<td>3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.</td>
<td>Yes</td>
<td></td>
<td>Non-privileged users are not permitted to execute privileged functions. Auditing of privileged functions is enabled.</td>
</tr>
<tr>
<td>3.1.8 Limit unsuccessful logon attempts.</td>
<td>No</td>
<td>(Recommendation) No domain exists so settings will be updated per system. Open Control Panel &gt; Administrative Tools</td>
<td></td>
</tr>
<tr>
<td>3.1.9 Provide privacy and security notices consistent with applicable CUI rules.</td>
<td>No</td>
<td>(Recommendation) No domain exists so settings will be updated per system. Open Control Panel &gt; Administrative Tools</td>
<td></td>
</tr>
<tr>
<td>3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.</td>
<td>No</td>
<td>(Recommendation) No domain exists so settings will be updated per system. Configure automatic session lock after a</td>
<td></td>
</tr>
<tr>
<td>3.1.11 Terminate (automatically) a user session after a defined condition.</td>
<td>No</td>
<td>(Recommendation) No domain exists so settings will be updated per system. Configure automatic session lock after a</td>
<td></td>
</tr>
</tbody>
</table>

**Implementation Dates:**

- 11/22/2017
- 11/24/2017
- 11/19/2017
- 11/25/2017
- 11/30/2017
- 12/9/2017
Secure Cyber Defense Compliance and Planning Engine (CAPE)

- Includes resources to achieve compliance
  - Incident Response Template
  - Maintenance Log
  - Media Control Log
  - Mobile Device Acceptable Use Policy
  - Risk Assessment
  - Visitor Log

- Each control is explained in plain language with selectable recommendation for each on how to achieve compliance

- Produces System Security Plan and POAM needed for 31 Dec 2017 deadline

- Expert security review within 24 hours of completion by our staff

- Only $995!!! $15K value!!!

- www.securecyberdefense.com/cape
Questions?

www.securecyberdefense.com
Cyber security economics analyzes the resources and time spent by the bad guys to break into a system versus resources and time spent by the good guys to protect, maintain, and recover. Relative time and/or effort is a fundamental metric.
DFARs Compliant while Empowering Your Business Process

With DoD approved Cloud For DFARs

FlowVU Solutions

Presentation by Eric Van Hoose
5 December 2017
1st Secure Cloud Success Story
AF Working with Their Contractors

mail responsible for 90% of cyber attacks

• Collaborate with Subs within Secure Cloud
• Team status of work 24/7 in secure folders
• Metrics for Team & Subs
• Process Improvement

Without using Email
1st Secure Cloud Success Story
AF Working with Selected Contractors*

Now Supporting AF Acquisition Process

AF Small Business Innovative Research Contracts*

AF Technology Acceleration Program*
1st Secure Cloud Success Story
Working with AF and 30 AFRL Contractors

3 Reasons Why It Works:

• 1st Its Secure meets DFARs requirements for DoD Approved Cloud

• 2nd Team can securely do work and store it in a secure folder (showing how it works in later)

• 3rd Securely communicate with Customer(s) Primes & suppliers,
Configured Milestones in Secure Folders
Secure Cloud Success Story
AF Working with Their SBIR Contractors

What’s next

- 1st **Detailed training** that includes getting you started

- 2nd **Help Desk** on an “as needed” basis for any specific problem

- 3rd **Configure Standard Process** to keep subs compliant
Working with AF Now*

*Small Business Innovation Research & Technology Acceleration Program

Website: flowvusolutions.com
Contact: Eric Van Hoose
937-531-6680, ext. 4122
evanhoose@vhainc.com
THANK YOU