Quick Start Strategy to Compliance

DFARS 252.204-7012

Rob Gillen
Overview

• 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. Policy and Personnel Assessment
  3. Technical Assessment
  4. System Security Plan (SSP) and Plan of Actions and Milestones (POA&M)
  5. Cloud-based Solutions
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
#1 Boundary Definition

• 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?
- 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
#2 Cybersecurity Policies

- 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 of 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
• 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.
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
Unicorn Supplies Manufacturing

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
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](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](http://www.securecyberdefense.com/cape)
What does SCD offer?

- **On-site/Remote assessment**
  - Includes an in-person or remote assessment of the organizations 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](mailto: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](mailto: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
Cybereconomics

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.

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
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 3Tenets 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
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.

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.

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.

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.
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 ie. Encrypt Devices

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

Encrypt all CUI for sending to Secure Cloud.
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.
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.
NIST 800-171 Compliance And Planning Engine

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.
Compliance Engine Instructions

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

Secure Cyber Defense, LLC - Miamisburg, OH 45342 - 937-388-4405
My Account

Hello camsilver (not camsilver? Log out)

From your account dashboard you can view your recent orders, manage your shipping and billing addresses and edit your password and account details.

My Memberships

<table>
<thead>
<tr>
<th>Plan</th>
<th>Start</th>
<th>Expires</th>
<th>Status</th>
<th>Next Bill On</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST 800-171 Compliance and Planning Engine Access</td>
<td>November 27, 2017</td>
<td>N/A</td>
<td>Active</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Secure Cyber Defense, LLC - Miamisburg, OH 45342 - 937-388-4405
Documents

- Incident Response Plan
- Maintenance Log
- Media Control Log
- Mobile Device Acceptable Use Policy
- Risk Assessment
- Visitor Log
CAPE

Step 1 of 112

Primary POC *
Shawn Walker

Email *
shawn.walker@secdfllc.com

Phone *
(937) 353-7504

Main company location *
31 South Second St
Street Address
Suite 202
Address Line 2
Miamisburg
City
45342
ZIP / Postal Code

State / Province / Region
OH
Country
United States

# of physical locations *
1

Please enter a value greater than or equal to 0.
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, or devices (including other information systems). *

- Yes
- No

Risk or Alternative Security Measures

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.
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

Step 24 of 132

24%

3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.

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

Are new employees made aware of the policies and standards of the Company? The training should be documented and validated by the trainer. A good template to use for security awareness training is here:
https://www.hhs.gov/about/agencyaffairs/cybersecurity/security-awards-training/index.html

Plan for compliance

- (Recommended) Build a process that all new employees must review all current Company policies and procedures. Create a log to track training that the employee must sign.
- Other

Date of implementation

07/15/2018
NIST 800-171 Compliance And Planning Engine

CAPE
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

9.13.32 Prohibit remote activation of collaborative computing devices (networked white boards/cameras/microphones) and provide indication of devices in use to users present at the device. *

☐ Yes
☐ No
☐ With an Alternative Security Measure

If collaborative computing devices are in use and networked, remote activation must be prohibited and configured to let users present at the device to see when it is in use. If you are not using collaborative computing devices, this is N/A.

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/A or an alternative security controls they will send it to the IAOB for review and approval.

No collaborative devices are in use at this facility.
CAPE
3.3 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

Sect 37 of 112

5.3.3 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

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

Have you configured auditing anywhere in your environment and are the logs being captured somewhere? Most company’s aren’t. So don’t panic, ideally you will want to implement a third-party tool which will save you a lot of time and headaches. There are free versions of auditing software as well that can be set up and implemented to help you with auditing in general. LDAP and NIS/LDAP have free versions that should be considered. Our recommendation will provide the specific items that should be audited. (“The version of NIS/LDAP we set is managed and fully functional”)

Plan for compliance

- [ ] Recommend auditing for active directory, firewall, servers, and any authentication that access company resources and/or data. Auditing policy should include login success/failure, logoff success/failure, security relevant directories success/failure, user or group rights privileges success/failure, system events success/failure, start or stop success/failure. Configure firewalls to forward egress traffic to a server. The location where the logs are stored is accessible to domain administrators only.
- [ ] CID - Managed Auditing
- [ ] Other

Date of implementation

Skip question for now  Skip to last page
## 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 cuhelp@securecyberdefense.com. Thank you!

<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>3.1.1 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><em>(Recommendation) Document and implement. Only users with approved user accounts shall be authorized access to the company network or data. Accounts shall be assigned by privileged users and will be unique to the user.</em></td>
<td>2017-11-22</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><em>(Recommendation) Create Security groups in Active Directory and assign those groups to applicable folders. Limit access permissions on individual folders if necessary.</em></td>
<td>2017-11-22</td>
</tr>
<tr>
<td>3.1.3 Control the flow of CUI in accordance with approved authorizations.</td>
<td>No</td>
<td><em>(Recommendation) Document the following policy: All CUI transmitted via email is encrypted and only sent to individuals with authorization to view the data. CUI is authorized within the organizational domain and not permitted for release to any other network or domain without prior authorization. Transmission of CUI outside the network is limited other than email encryption is prohibited.</em></td>
<td>2017-11-22</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><em>(Recommendation) Admin account access will be limited to privileged users who will be identified in writing.</em></td>
<td>2017-11-24</td>
</tr>
<tr>
<td>3.1.8 Limit unsuccessful login attempts.</td>
<td>No</td>
<td><em>(Recommendation) No domain exist so settings will be updated per system. Open Control Panel &gt; Administrative Tools &gt; Local Security Policy. Set Account Policies &gt; Account Lockout Policy. Set account lockout duration to 5, Account lockout threshold to 5, and Reset account lockout counter after 5.</em></td>
<td>2017-11-19</td>
</tr>
</tbody>
</table>
# 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 cybersecurity@securecyberdefense.com.

Thank you!

### Plan of Action

<table>
<thead>
<tr>
<th>NIST 800-171 Control</th>
<th>Compliant</th>
<th>Method of 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 malicious activity without collusion.</td>
<td>Yes</td>
<td>Personnel designated to review and monitor audit logging and logs are explicitly defined. Only they have rights to access the audit log and server.</td>
<td></td>
</tr>
<tr>
<td>3.1.5 Use non-privileged accounts or roles when accessing nonessential functions.</td>
<td>Yes</td>
<td>Only non-admin accounts are permitted to log in to perform everyday nonessential related activities. The use of admin accounts is audited and monitored.</td>
<td></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>Non-privileged users are not permitted to execute privileged functions. Auditing of privileged functions is enabled.</td>
<td></td>
</tr>
<tr>
<td>3.1.14 Route remote access via managed access control points.</td>
<td>Yes</td>
<td>Remote access is directed through the firewall.</td>
<td></td>
</tr>
<tr>
<td>3.1.16 Authorize wireless access prior to allowing such connections.</td>
<td>Yes</td>
<td>Wireless access is permitted to policy. The specific rules for using the wireless connection are defined.</td>
<td></td>
</tr>
<tr>
<td>3.1.17 Protect wireless access using authentication and encryption.</td>
<td>Yes</td>
<td>Wireless protected by WPA2 encryption. Only organizational users are able to authenticate to the wireless connection.</td>
<td></td>
</tr>
<tr>
<td>3.1.20 Leech and control limited connections to and use of external information systems.</td>
<td>Yes</td>
<td>Policy is in place that provides connections to external systems from the organizational network. Policy also defines how and when users are permitted to use external systems to access Company data.</td>
<td></td>
</tr>
<tr>
<td>3.1.22 Control information posted or processed on publicly accessible information systems.</td>
<td>Yes</td>
<td>Personnel who are permitted to post information to publicly accessible systems are authorized in writing. They are the only ones with the rights necessary to post updates. They are also</td>
<td></td>
</tr>
</tbody>
</table>
# 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 care@securecyberdefense.com. Thank you!

## Plan of Action

<table>
<thead>
<tr>
<th>NIST 800-171 Control</th>
<th>Compliant</th>
<th>Method of compliance</th>
<th>Estimated implementation date</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6.8 Implement cryptographic mechanisms to protect the confidentiality of data stored on digital media during transport unless otherwise protected by alternative physical safeguards.</td>
<td>No Alternative Security Measure</td>
<td>Policy documented that all data transferred out of the physical workplace is accompanied using two-person integrity.</td>
<td></td>
</tr>
<tr>
<td>3.13.6 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.</td>
<td>No Alternative Security Measure</td>
<td>No publicly accessible systems in this organization.</td>
<td></td>
</tr>
<tr>
<td>3.13.12 Protect remote activation of collaborative computing devices/components while (transmitting/microphones) and provide indication of devices in use to users present at the device.</td>
<td>No Alternative Security Measure</td>
<td>No collaborative computing devices in use in the organization.</td>
<td></td>
</tr>
</tbody>
</table>
## 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 culming@set.com or cyberdefense.com

Thank you!

### Plan of Action

<table>
<thead>
<tr>
<th>NIST 800-171 Control</th>
<th>Compliant</th>
<th>Plan for compliance</th>
<th>Method of compliance</th>
<th>Estimated implementation date</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1 Limit information system access to authorized users, process access 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 company network or site. Accounts will be assigned to privileged users and will be unique to the user</td>
<td>2017-11-22</td>
<td></td>
</tr>
<tr>
<td>3.1.2 Limit intra-system access to the type of transactions and functions that authorized areas are permitted to execute.</td>
<td>No</td>
<td>(Recommendation) Create Security groups in Active Directory and assign those groups to applicable folders. Lift down permissions on individual folders as necessary.</td>
<td>2017-11-22</td>
<td></td>
</tr>
<tr>
<td>3.1.3 Ensure the flow of CIA in accordance with established authorizations.</td>
<td>No</td>
<td>(Recommendation) Document the current policy for CIA transferred via email in a Controlled Unclassified Environment (CUE). Implement controls to ensure that only authorized users have access to the email.</td>
<td>2017-11-22</td>
<td></td>
</tr>
<tr>
<td>3.1.4 Separate the duties of individuals to reduce the risk of noncompliant activity without collusion.</td>
<td>Yes</td>
<td>None</td>
<td>Personnel designated to review and monitor audit logging activities are responsible for ensuring that they have the right access to the audit logs and that audits are conducted</td>
<td></td>
</tr>
<tr>
<td>3.1.5 Employ the principle of least privilege, including the following:</td>
<td>No</td>
<td>(Recommendation) Allow account access will be limited to privileged access which will be identified in writing.</td>
<td>2017-11-24</td>
<td></td>
</tr>
<tr>
<td>NIST 800-171 Control</td>
<td>Compliant</td>
<td>Plan for compliance</td>
<td>Method of compliance</td>
<td>Estimated implementation date</td>
</tr>
<tr>
<td>----------------------</td>
<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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/22/2017</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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/22/2017</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 personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/22/2017</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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/24/2017</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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/24/2017</td>
</tr>
<tr>
<td>3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.</td>
<td>Yes</td>
<td></td>
<td>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/24/2017</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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/24/2017</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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/19/2017</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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>11/25/2017</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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>12/30/2017</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>Personnel designated to review and monitor audit logging and tools are explicitly defined. Only they have rights</td>
<td>12/9/2017</td>
</tr>
</tbody>
</table>
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](http://www.securecyberdefense.com/cape)
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?

Demo
DFARs Compliant while Empowering Your Business Process

With DoD approved Cloud For DFARs
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,
For SBIR Contractors

Demo

Screen Shots
Tuesday, 5 December, 2017
Configured Milestones in Secure Folders
Secure AdHoc Workflows
Simple as Emails But More Secure
Secure Cloud Success Story
AF Working with Their SBIR Contractors
What’s next

• 1\textsuperscript{st} Detailed training that includes getting you started

• 2\textsuperscript{nd} Help Desk on an “as needed” basis for any specific problem

• 3\textsuperscript{rd} 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