

FUSION₁₇

DRIVING SERVICE MANAGEMENT FORWARD

DFARS 252 Assessment

Session 208: NIST SP 800-171 and Controlled Unclassified Information

Presented by:

Miguel (Mike) O. Villegas, CISA, CISSP, CSX|F, PA QSA, PCI QSA
734-546-9605
mike.villegas@k3des.com

PRODUCED BY: **HDI itSMF USA** | **#SMFUSION**

Who does this apply to?

- ❖ Non-Federal Information System – an information system used to operate by a non-federal organization that stores, processes, or transmits CUI (See NIST SP 800-171r1)
- ❖ Non-Federal Organizations – federal contractors; state, local, and tribal governments; and colleges and universities
- ❖ Ask your federal contractor such as Raytheon, Boeing, Lockheed...

Questions:

- Does this apply to me?
- I am being asked to be DFARS compliant but from my:
 - Partners
 - Customers
 - Federal Contractor (not one of the primes)
- Will the date (12/31/17) change? It is now November 2017.
- I have been asked to complete the Exostar form online. Isn't that all I need to do?
- I'm a university, bank, manufacturer, public utility, etc. I am not a defense contractor. Does this apply to me? Or does it?
- I can't believe they would cut my contract if not compliant. How serious is this?

On September 14, 2016, NIST SP 800-171r1 (Controlled Unclassified Information in Nonfederal Information Systems and Organizations) was formally issued to provide guidance on controlled unclassified information (CUI).

Safeguarding or disseminating CUI, consistent with applicable law, regulations, and government-wide policies, is vital, and noncompliance by **December 31, 2017**, means government contractors will lose their contract.

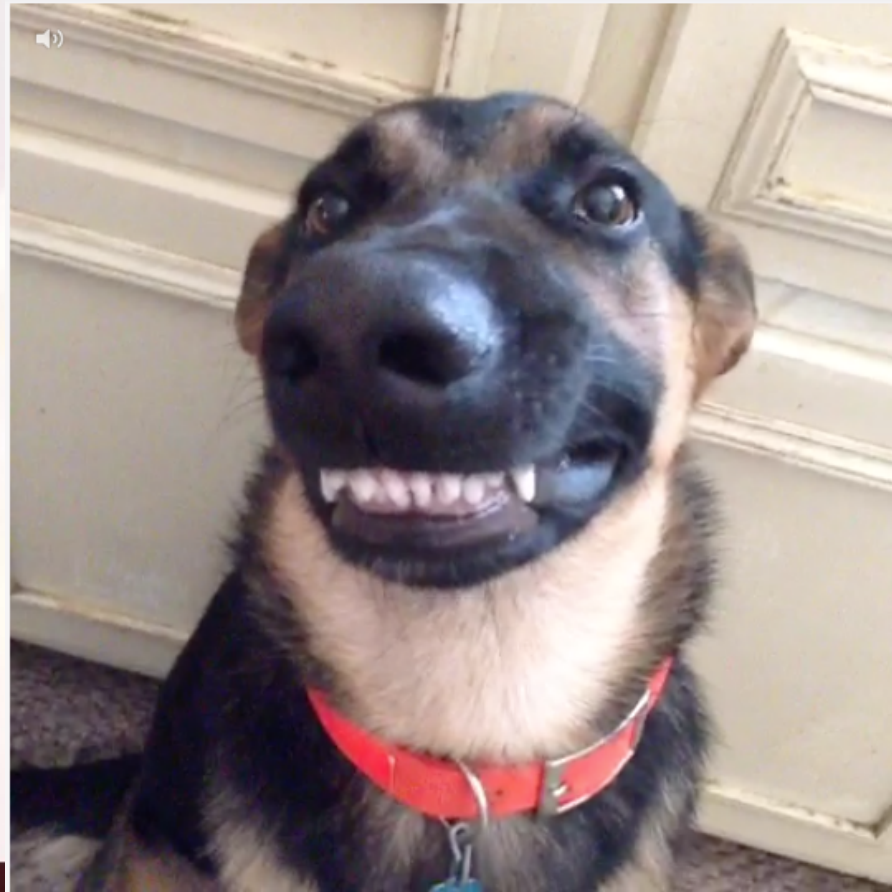
Experience has shown that this order, like others before it, will not be taken seriously—but it should be. If your organization is facing noncompliance, this session will focus on the NIST SP 800-171 control families, requirements, and compliance dates.

On September 14, 2016, NIST SP 800-171r1 (Controlled Unclassified Information in Nonfederal Information Systems and Organizations) was formally issued to provide guidance on controlled unclassified information (CUI).

Safeguarding or disseminating CUI, consistent with applicable law, regulations, and government-wide policies, is vital, and noncompliance by **December 31, 2017**, means government contractors will lose their contract.

Experience has shown that this order, like others before it, will not be taken seriously—but it should be. If your organization is facing noncompliance, this session will focus on the NIST SP 800-171 control families, requirements, and compliance dates.

Chief Information Security Officer (CISO)



What is DFARS?

DFARS - Defense Federal Acquisition Regulation Supplement

DFARS **252.204-7012**
protect Controlled U
incidents



cy requirements to
report security

Controlled Unclassified Information (CUI) Registry

- ❖ Agriculture
- ❖ Controlled Technical Information
- ❖ Critical Infrastructure
- ❖ Emergency Management
- ❖ Export Control
- ❖ Financial
- ❖ Geodetic Product Information
- ❖ Immigration
- ❖ Intelligence
- ❖ International Agreements
- ❖ Law Enforcement
- ❖ Legal
- ❖ NATO
- ❖ Nuclear
- ❖ Privacy
- ❖ Procurement and Acquisition
- ❖ Financial
- ❖ Proprietary Business Information
- ❖ SAFETY Act Information
- ❖ Statistical
- ❖ Tax
- ❖ Transportation

<https://www.archives.gov/cui/registry/category-list#page-header>

What is NIST SP 800-171r1?

The cybersecurity framework specified under DFARS 252.204-7012. Derived from NIST SP 800-53r4 and FIPS 200. Consists of 14 Control Families and 110 Controls

| | |
|----|--------------------------------------|
| AC | ACCESS CONTROL |
| AT | AWARENESS AND TRAINING |
| AU | AUDIT AND ACCOUNTABILITY |
| CA | SECURITY ASSESSMENT |
| CM | CONFIGURATION MANAGEMENT |
| IA | IDENTIFICATION AND AUTHENTICATION |
| IR | INCIDENT RESPONSE |

| | |
|----|--------------------------------|
| MA | MAINTENANCE |
| MP | MEDIA PROTECTION |
| PS | PERSONNEL SECURITY |
| PE | PHYSICAL PROTECTION |
| RA | RISK ASSESSMENT |
| SC | SYSTEM & COMMUNICATIONS |
| SI | SYSTEM & INFORMATION INTEGRITY |

CUI Security Requirements

- ❖ NIST SP 800-171r1 is made up of basic and derived security requirements are obtained from FIPS 200 and NIST SP 800-53, respectively
- ❖ NIST SP 800-171r1 is made up of 14 Families of controls.

| NIST SP 800-171 Chapter Three | | | | | |
|---|------------------------|--------|-------------------------------|------------|--|
| THE REQUIREMENTS | | | | | |
| SECURITY REQUIREMENTS FOR PROTECTING THE CONFIDENTIALITY OF CUI | | | | | |
| 800-171 Section | 800-171 Control Family | Symbol | Requirement Type | Procedures | Testing Procedure |
| 3.1 | ACCESS CONTROL | AC | Basic Security Requirements | 3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. |
| 3.1 | ACCESS CONTROL | AC | Derived Security Requirements | 3.1.3 | Control the flow of CUI in accordance with approved authorizations. |
| 3.1 | ACCESS CONTROL | AC | Derived Security Requirements | 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. |
| 3.1 | ACCESS CONTROL | AC | Derived Security Requirements | 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. |
| 3.1 | ACCESS CONTROL | AC | Derived Security Requirements | 3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions. |
| 3.1 | ACCESS CONTROL | AC | Derived Security Requirements | 3.1.7 | Prevent non-privileged users from executing privileged functions and audit the execution of such functions. |
| 3.1 | ACCESS CONTROL | AC | Derived Security Requirements | 3.1.8 | Limit unsuccessful logon attempts. |

Source: Dr. Ron Ross, NIST

Definitions

- OEM - **original equipment manufacturer** (OEM) is a company whose products are used as components in the products of another company, referred to as the value-added reseller (VAR)
- **Federal contractors** are individuals or employers who enter into a contract with the United States (any department or agency) to perform a specific job, supply labor and materials, or for the sale of products and services.
- [Top 100 Contractors](#) – the top 100 contractors in 2015 included, Lockheed Martin Corp, The Boeing Company, General Dynamics Corp, Raytheon Company, Northrop Grumman Corporation, McKesson Corporation, United Technologies Corporation, and many more. These are typically the PRIMARY CONTRACTOR with a government agency.
- Government Agency – The top five departments by dollars obligated in 2015 were the [Department of Defense](#) (\$212.5 billion), [Department of Energy](#) (\$23 billion), [Health and Human Services](#) (\$21 billion), [Department of Veteran Affairs](#) (\$20 billion), and [NASA](#) (\$13 billion)
- DAA - The **Designated Approving Authority**, (e.g, in the [United States Department of Defense](#)), is the official with the [authority](#) to formally assume [responsibility](#) for operating a system at an acceptable level of [risk](#). The new official term that has replaced DAA is Authorizing Official (AO).

Definitions (continued...)

- ❖ What Are The Differences Between The Accreditation Decisions? Once the Designated Approval Authority (DAA) has reviewed the system information and recommendation, there are four possible DAA accreditation decisions that can be made:
 - ❖ Authorization to Operate (ATO) – full operation approval with a duration of three years;•
Interim Authorization to Operate (IATO) – allows operation to manage IA security weaknesses for a maximum of six months ;
 - ❖ Interim Authorization to Test (IATT) – a special case for authorizing testing allowing operation for a limited time; or
 - ❖ Denial of Authorization to Operate (DATO) – issued if a DoD information system has inadequate IA design. If you receive a DATO, please contact your organization’s Information Assurance (IA) professional.

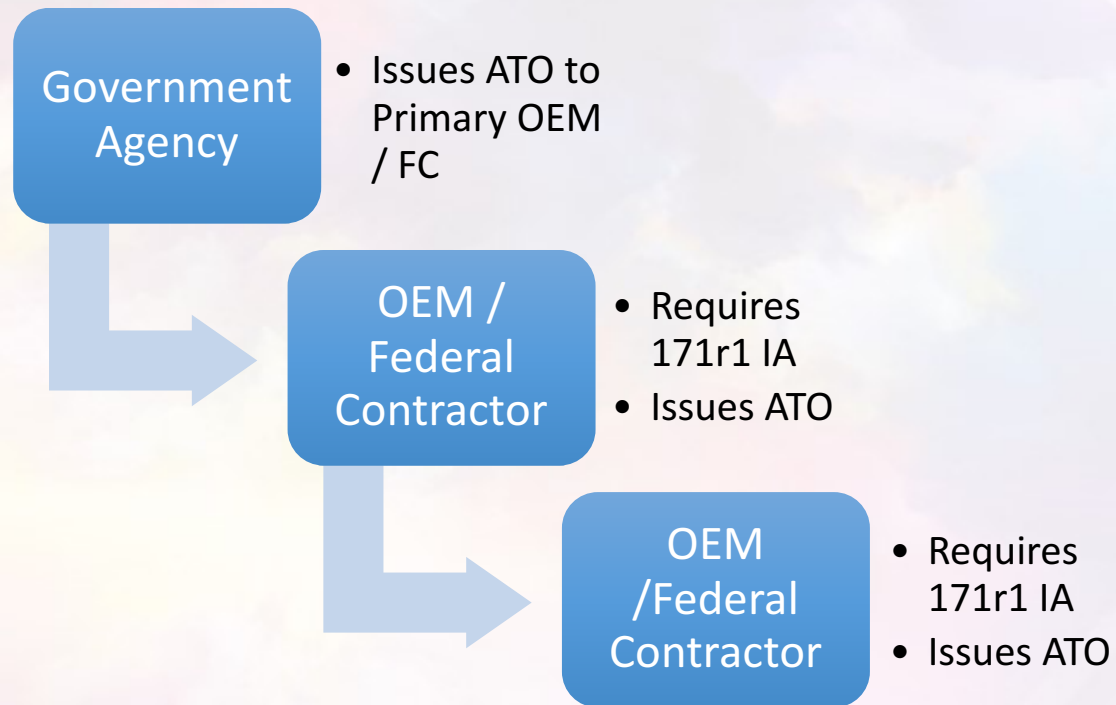
NOTE: If an Accreditation Decision has not been issued, a system is considered “unaccredited” and is not allowed to operate.

- ❖ NIST Special Publication 800-171 r1 – formally issued completed on December 20, 2016

Definitions (continued...)

- ❖ IA – Information assessment
- ❖ Federal Information System – an information system used to operate by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (See Federal Information Security Management Act (FISMA) – 40 U.S.C., Sec. 11331)
- ❖ Non-Federal Information System – an information system used to operate by a non-federal organization that stores, processes, or transmits CUI (See NIST SP 800-171r1)
- ❖ Non-Federal Organizations – federal contractors; state, local, and tribal governments; and colleges and universities
- ❖ POAM - plans of action and milestones (POAM) for any planned implementations or mitigations
- ❖ SSP - Nonfederal organizations describe in a system security plan (SSP), how the CUI requirements are met or how organizations plan to meet the requirements. The SSP describes the boundary of the information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems.

Road to ATO



Definitions (continued...)

- ❖ [NIST Special Publication 800-171 r1](#) – formally issued completed on December 20, 2016. This publication provides federal agencies with a set of recommended security requirements for protecting the confidentiality of **CUI** when such information is resident in nonfederal systems and organizations.
- ❖ **CUI** – Controlled Unclassified Information - is any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.
- ❖ [CUI Registry](#) - is the online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent.
- ❖ **Information technology** - (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, Defense Federal Acquisition Regulation Supplement management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency

Why does any of this matter?



Which supply chains are affected?



GENERAL DYNAMICS

Raytheon



MCKESSON

NORTHROP GRUMMAN

Boeing Commercial Airplanes supply chain

1 billion parts procured per year



\$43 billion spend • 5,400 factories • 500,000 people



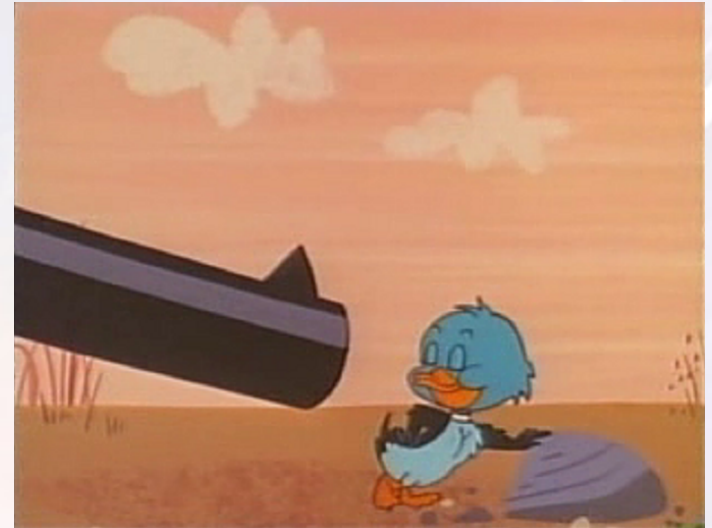
Industries Affected by DFARS

- ❖ Manufacturing – direct to Primes or Tertiary Contractors
- ❖ Universities with Government Grants – Defense Research
- ❖ Non-Federal Information System – an information system used to operate by a non-federal organization that stores, processes, or transmits CUI (See NIST SP 800-171r1)
- ❖ Non-Federal Organizations – federal contractors; state, local, and tribal governments; and colleges and universities

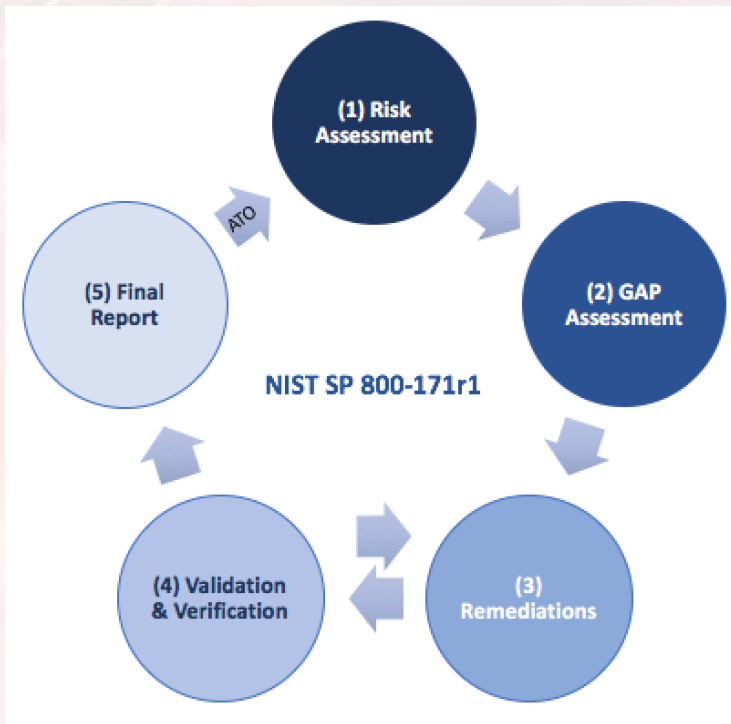
<https://www.archives.gov/cui/registry/category-list#page-header>

Why do so many of these firms have so few cybersecurity measures in place?

No ROI +



Approach



PHASE 1 – Risk Assessment – this is a scoping exercise to determine what 171r1 test procedures apply for this assessment; need Pre-Assessment Questionnaire; address only moderate and higher impacts based on FIPS 199

PHASE 2 – Gap Assessment – test each in-scope 171r1 test procedures; state whether compliant or is a gap with recommended remediations

PHASE 3 – deploy or facilitate remediations for open gaps; refer to appropriate managed service providers; develop POA&M for each major gap and an overall SSP

PHASE 4 – test, validate and verify that remediations have been implemented properly and support compliance to 171r1

PHASE 5 – complete the Final NIST SP 800 171r1 report stating client is fully compliant

Phase 1 – Risk Assessment

- ❖ **PHASE 1** – Risk Assessment – this is a scoping exercise to determine what 171r1 test procedures apply for this assessment
 - ❖ Pre-Assessment Questionnaire
 - ❖ Create SOW and obtain signed agreement
 - ❖ Complete FIPS 199
 - ❖ address only moderate and higher impacts based on FIPS 199
 - ❖ NIST SP 800-171r1-PBC.docx

Pre-Assessment Questionnaire

Look at DFARS-Assessment_Questionnaire_2017.docx in the Dropbox folder.

Based on the results of the Pre-Assessment Questionnaire, the primary (MMTV, CMTC, Alvaka, etc.), will put together an RFQ, SOW, or proposal based on what is requested or agreed to with the client.

Each primary needs to run the proposed fee with MMTV (assessor) BEFORE committing to client. The reason is because the amount of work to perform Phase 1 and Phase 2 needs to be determined by the assessor, not the primary. This is reciprocated when the assessor recommends Alvaka or another remediator to the client to address a gap.

Basic Guideline: The less the client has in place (“No”) answers in the Pre-Assessment Questionnaire, the less the effort to develop a Gap Assessment (Phase 1 and 2). The more they have in place, the more testing is required to determine where they are compliant and what remediations will address the gaps. Testing of controls takes place in Phase 2 and Phase 4.

FIPS 199

FIPS 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

- ❖ The *potential impact* is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
- ❖ The *potential impact* is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals
- ❖ The *potential impact* is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The generalized format for expressing the security category, SC, of an information type is:

SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE

Only those impacts that are moderate and high are in-scope of the NIST SP 800-171r1 IA. (See [fips_199_security_categorization.docx](#))

Phase 2 – Gap Assessment

- ❖ **PHASE 2** – Gap Assessment – test each in-scope 171r1 test procedures; state whether compliant or is a gap with recommended remediations
 - ❖ CSET 8.0
 - ❖ NIST SP 800-171r1 Worksheet
 - ❖ Use NIST SP 800-171r1 Folder Structure for Evidence
 - ❖ Test, Verify, and Evidence all In-Scope Test Procedures
 - ❖ Recommend viable, cost effective, risk based remediations that satisfy test procedure and control
 - ❖ Identify compensating control (CC) if remediation is too expensive, time consuming, or not feasible; but **only** if the CC will satisfy the test procedure
 - ❖ Gap Assessment and Risk Assessment must be QA'd by primary and assessor management team **before** delivered to client

CSET®

CYBER SECURITY EVALUATION TOOL

Version 8.0

Prepare Your Assessment

CSET helps you determine the cybersecurity posture of your organization as you answer questions based on recognized industry standards about your systems and procedures.

Before you can answer questions, your question set needs to be identified. The 'Start Here' button begins the question identification and preparation process.

Start Here >>

 Preparation ▾

 Assessment ▾

 Results ▾

 Diagram



Site Information

Please enter information about your assessment, including the assessment name and date. The facility and contact information sections are optional. DOD customers should complete the DOD eMASS section.

Assessment Name

Assessment Date



Facility Name

City or Site Name

State, Province, or Region

Optional DOD eMASS Specific Information ▾

Assessor Name

Assessor Email

Assessor Telephone

Contacts

[Manage Contacts](#)

Name ▲

Job Title ▲

Organization ▲

[< Back](#)

[Continue >>](#)

Sector and Demographic Information

Please select your sector, industry, and answer the questions below to help identify the final question set for your assessment.

Sector

Not Selected

- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

protect?
nt?

- Privacy is a significant concern for the assets I am trying to protect.
- I am concerned about supply chain cybersecurity management.
- My organization uses industrial control systems (ICS).

< Back

Continue >>

Access Control

Access Agreements

Do you have any access agreements (formal or informal) for third party access to your system? Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, operational or service level agreements and conflict-of-interest agreements.

- Yes No Not Applicable Override

- 1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?
- 2 Are access agreements periodically reviewed and updated?

Access Enforcement

3 Does the system enforce assigned authorizations for controlling electronic access to the system?

- Yes
 No
 Not Applicable
 Alternative Response

Supplemental Information

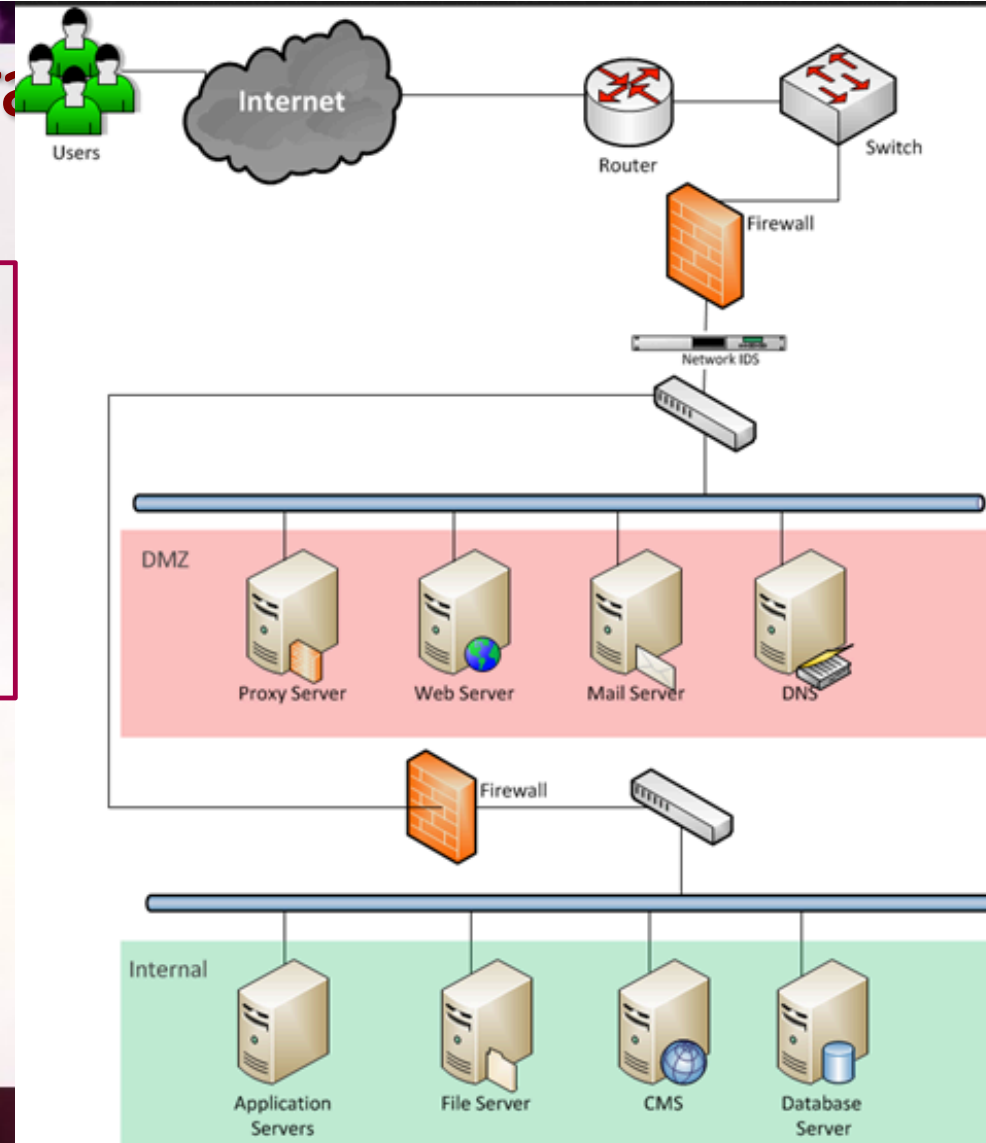
2.15 Access Control
The focus of access control is ensuring that resources are only accessed by the appropriate personnel and that personnel are correctly identified. The first step in access control is creating access control lists with access privileges for personnel. The next step is to implement security mechanisms to enforce the access control lists. Mechanisms also need

[Read more...](#)

Network Diagram

This is a simple network diagram that demonstrates a pictorial view of the network topology, components, segmentation, and firewall / router / switch / IDS placements.

This network diagram must coincide with actual layer 3 configurations and rules (ACLs and VLANs).



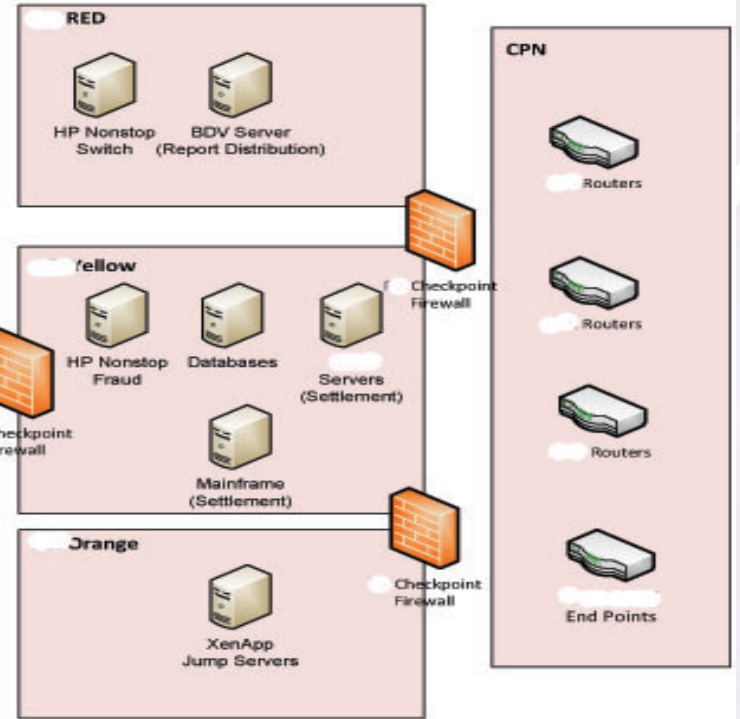
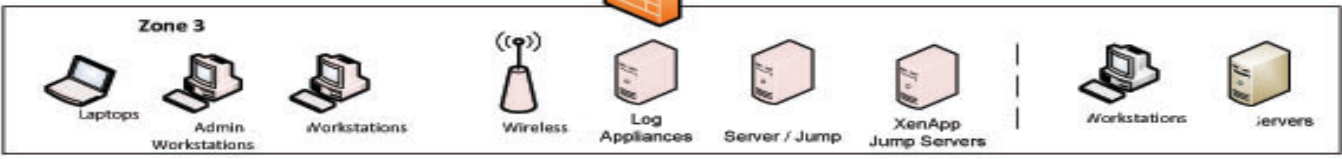
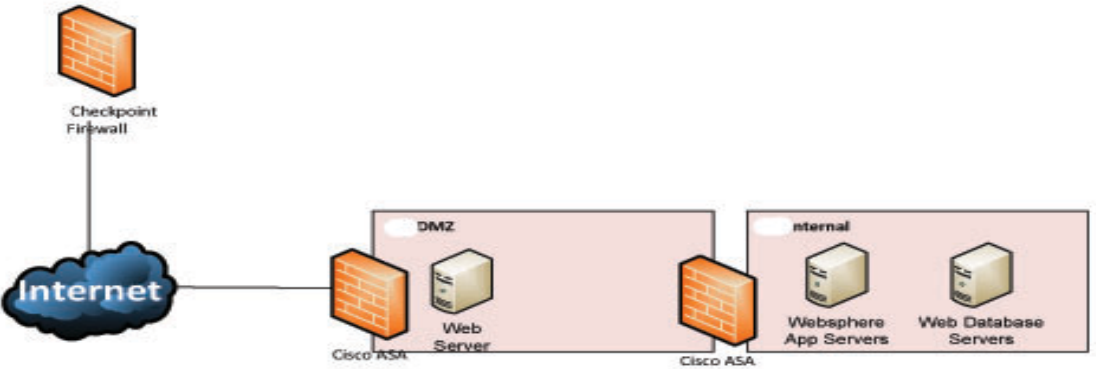
Network Diagram With Segmentation



Network Diagram Sample (Redacted)

Infrastructure

In Scope Not In Scope



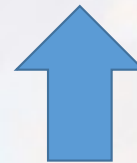
Compensating Controls

Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:

1. Meet the intent and rigor of the original control;
2. Provide a similar level of defense as the original control
3. Be “above and beyond” other control requirements (not simply in compliance with other control); and
4. Be commensurate with the additional risk imposed by not adhering to the control

Source: PCI DSS v3.2

Phase 3 - Remediations



Phase 4 – Validation and Verification

Monitoring Tools

- SIEM – Security Incident & Event Monitor
- IPS/IDS – Intrusion Prevention/Detection System
- WAF – Web Application Firewall
- Database Monitoring
- Multi-Factor Authentication
 - Hard Tokens
 - Soft Tokens
- Network Monitoring
- TLS/SSL/EV – Web communication encryption
- Data Loss Prevention (DLP)

Magic Quadrant



A GOOD START

- Gardner Magic Quadrant
- Forrester Wave

**DON'T RECOMMEND A CADILLAC
IF
A CHEVY TRUCK WILL DO**

Security Information & Event Monitor (SIEM)

COMMERCIAL



OPEN SOURCE



- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures
- Agent and/or Agentless

File Integrity Monitoring

COMMERCIAL



OPEN SOURCE

TRIPWIRE



AIDE

- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures

IDS/IPS

COMMERCIAL



OPEN SOURCE



- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures

Web Application Firewalls

COMMERCIAL



OPEN SOURCE



ESAPI Web Application Firewall (ESAPI WAF)



- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current attack vendors

Database Monitoring

COMMERCIAL



OPEN SOURCE



- Cost
- Scalability
- Flexibility
- Skill set requirements
- Current signatures
- Agent and/or Agentless

Multi-Factor Authentication

- Multi-factor authentication (also Multi-factor authentication, MFA, or M-FA) is an approach to authentication which requires the presentation of two or more of the three authentication factors
 - Something I know
 - Something I have
 - Something I am

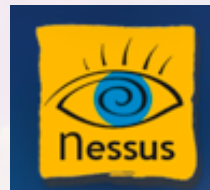


- RSA SecurID



PhoneFactor offers instant integration with a wide range of applications, including all leading remote access VPN solutions, single sign-on systems, cloud applications, online banking, and websites as well as custom applications. PhoneFactor also integrates with Active Directory and LDAP servers for centralized user management.

Networking Monitoring

The logo for GFI, featuring the letters "GFI" in a bold, blue, sans-serif font with a registered trademark symbol.The logo for Check Point Software Technologies Ltd., featuring a small icon of a computer monitor with a red and blue graphic, followed by the text "Check Point" in a large, bold, black font and "SOFTWARE TECHNOLOGIES LTD." in a smaller, black font below it.The logo for Barracuda Networks, featuring a stylized blue and white fish-like shape with the word "BARRACUDA" in a bold, blue font and "NETWORKS" in a smaller, white font below it.The logo for Splunk, featuring the word "splunk" in a white, lowercase, sans-serif font on a black rectangular background.The logo for Nessus, featuring a yellow square with a blue eye-like graphic and the word "Nessus" in a black font below it.The logo for Qualys On Demand Security, featuring a red shield with a white "Q" inside, followed by the word "QUALYS" in a bold, black font and "ON DEMAND SECURITY" in a smaller, black font below it.The logo for Trustwave, featuring a blue and green stylized wave icon followed by the word "Trustwave" in a blue font with a registered trademark symbol.The logo for Rapid7, featuring the word "RAPID" in a bold, black font and "7" in a bold, orange font.The logo for IBM, featuring the word "IBM" in a bold, black font with horizontal stripes.

- **A detailed analysis of vulnerabilities** found within your IP addresses or domain, classified by High, Medium or Low severity
- **Step-by-step instructions on how to remediate threats**, so you can immediately address the most serious vulnerabilities

Data Loss Prevention



websense®

DLPWorks.com
Code Green Networks Authorized Reseller



RSA



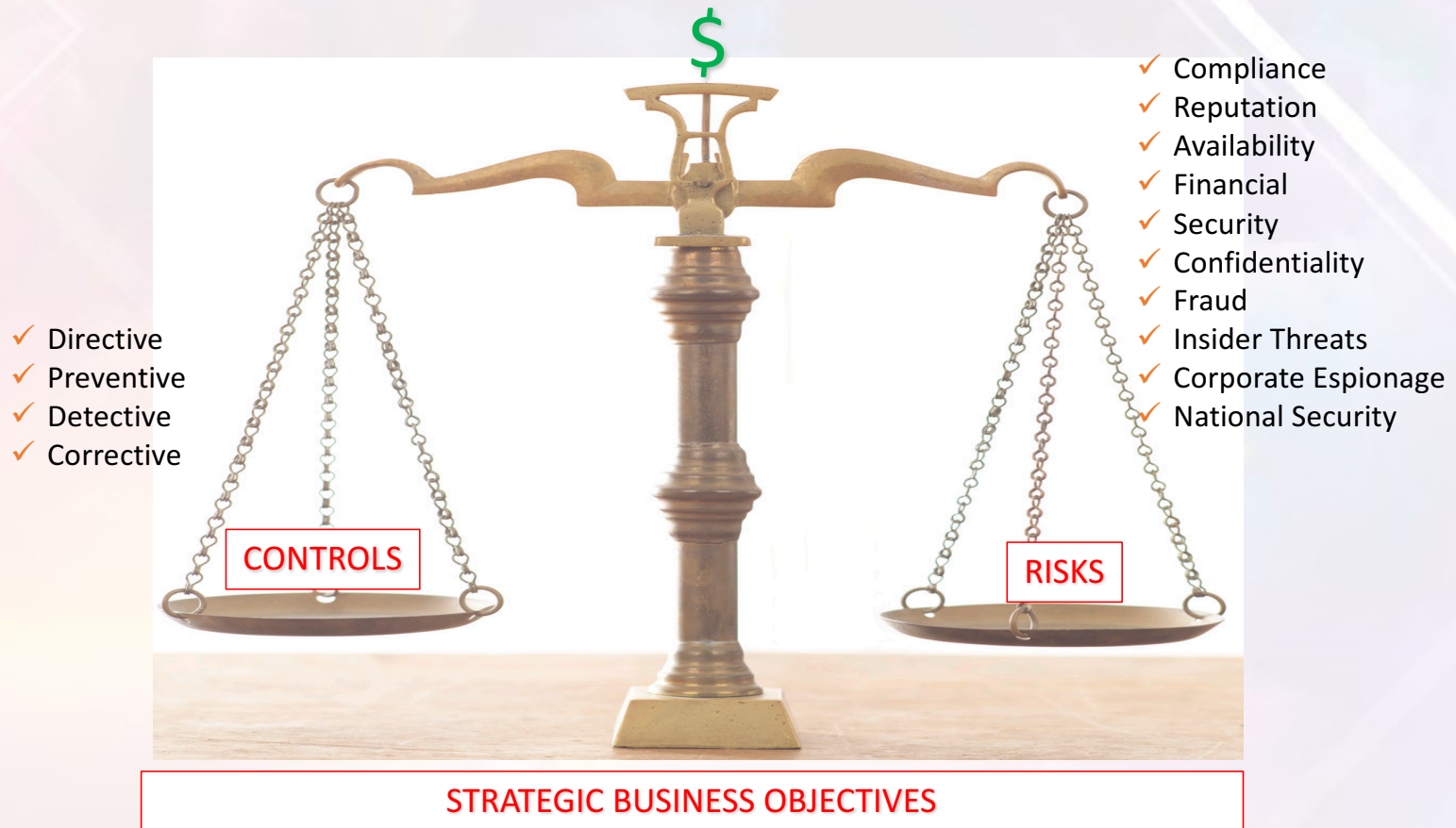
 **Trustwave®**

MY DLP

opendlp

- Detect, block or control the usage of (for example, saving, printing or forwarding) specific content based on established rules or policies.
- Monitor network traffic for, at a minimum, e-mail traffic and other channels/protocols (HTTP, IM, FTP) and analyze across multiple channels, in a single product and using a single management interface.
- End-Point / Network / Discovery

Balanced View of Information Security



PHASE 5 – complete the Final DFARS/ NIST SP 800 171r1 report stating client is fully complia

Complete the Exostar and state you either compliant or not.

If not, you then need to provide:

- Systems Security Plan (SSP)
- Plan of Action and Milestone (POA&M) for each gap
 - Each gap needs a plan
 - Each gap needs a timeline and deadline
 - Make sure you meet that deadline

Caveats?

GAP Assessment prior to Risk Assessment
will miss the target



NIST SP 800-171r1 IT and OT Considerations

- general purpose information systems;
- industrial and process control systems;
- cyber-physical systems; and
- individual devices that are part of the *Internet of Things*.

Shop Floor & SCADA systems are in scope

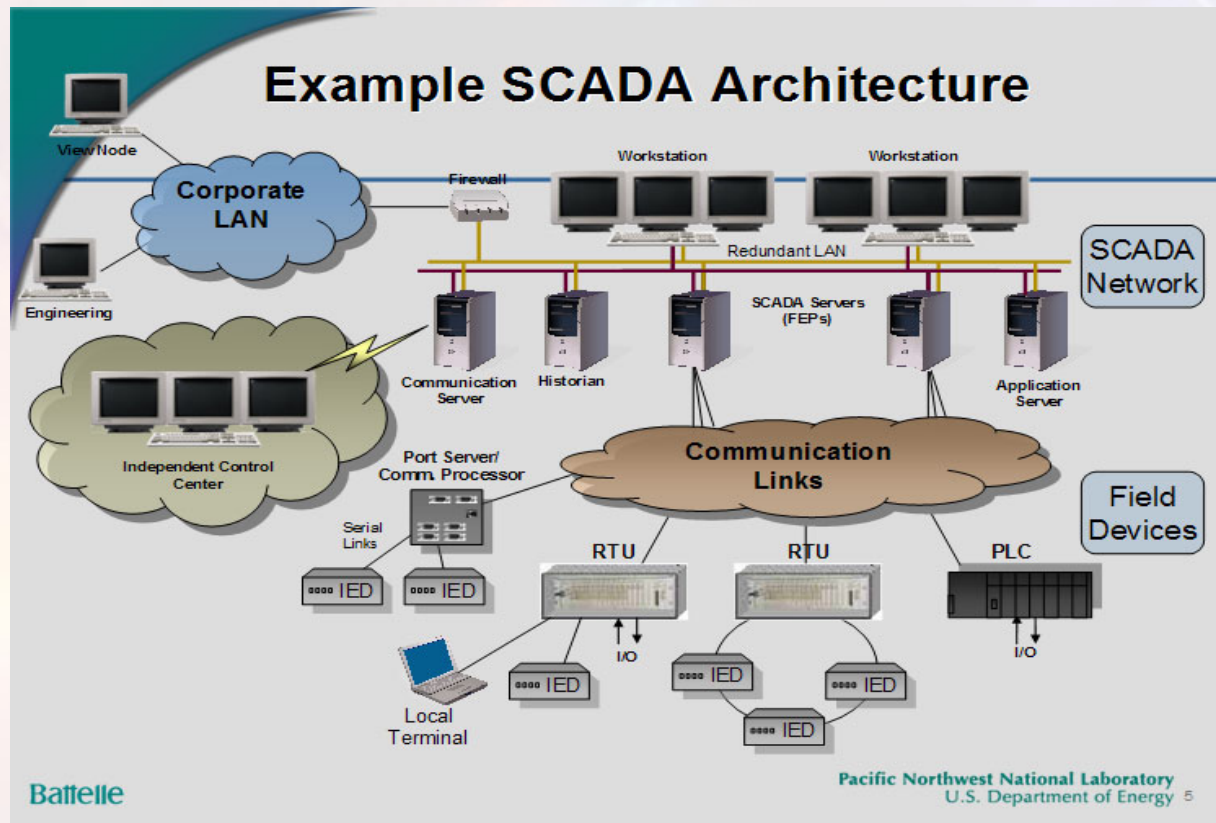


Table AP3.T2 DoD Approved Baseline Certifications

| IAT Level I | | IAT Level II | | IAT Level III | |
|--|--|---|--|--|--|
| A+-CE Network+ CE SSCP CCNA-Security | | GSEC Security+ CE SSCP CCNA-Security | | CISA GSE GCIH GCED CISSP (or Associate) CASP | |
| IAM Level I | | IAM Level II | | IAM Level III | |
| CAP GIST GSLC Security+ CE | | CAP GSLC CISM CASP CISSP (or Associate) | | GSLC CISM CISSP (or Associate) | |
| IASAE I | | IASAE II | | IASAE III | |
| CISSP (or Associate) CASP CSSLP | | CISSP (or Associate) CASP CSSLP | | CISSP - ISSEP CISSP - ISSAP | |
| CNDSP Infrastructure Support | | | | | |
| CNDSP Analyst | | CNDSP Incident Responder | | CNDSP Auditor | |
| GCIA CEH GCIH | | SSCP CEH | | GCIH CSIH CEH GCFA | |
| | | | | CNDSP Manager | |
| | | | | CISA GSNA CEH | |
| | | | | CISSP-ISSMP CISM | |

Mike O. Villegas, CISA, CISSP, GSEC, CSX|F, PCI-QSA, PA-QSA

Miguel (Mike) O. Villegas is a Senior Vice President for K3DES LLC. He performs and QA's PCI-DSS and PA-DSS assessments for K3DES clients. He also manages the K3DES ISO/IEC 27002:2013 program. Mike also specializes in DFARS 252/NIST SP 800-171r1 compliance. He was previously Director of Information Security at Newegg, Inc. for five years. Mike currently is a Contributing Writer for SearchSecurity.com –TechTarget with over published 150 articles.

Mike has over 35 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Arthur Andersen and Ernst & Young for their information systems security and IS audit groups over a span of nine years. Mike is a CISA, CISSP, GSEC, PCI-QSA and PA-QSA.

Mike was president of the LA ISACA Chapter during 2010-2012 and president of the SF ISACA Chapter during 2005-2006. He was the SF Fall Conference Co-Chair from 2002–2007 and also served for two years as Vice President on the Board of Directors for ISACA International. Mike has taught CISA review courses for over 20 years.

Summary Steps

1. Asses Legal & Contractual Requirements
2. Start with a DFARS Scoping & Readiness Assessment
3. Author Policy and Procedures
4. Implement Technical Remediation Measures as Needed
5. Institute Security Awareness and Training
6. Perform an Annual Risk Assessment
7. Confirm Successful Remediation Efforts
8. Ensure System Security Plan (SSP) and other Related Documents are in Order
9. Have an Independent Party perform an Assessment for DFARS compliance
10. Engage in Continuous Monitoring of your controls
11. Know that Federal Compliance is here to stay
12. Remember you have until December 31, 2017 to be compliant!

FUSION₁₇

DRIVING SERVICE MANAGEMENT FORWARD

Thank you for attending this session.

***Please complete the session evaluation form
SMFusion.com/Feedback or on the **FUSION App**.***

PRODUCED BY: **HDI** *itSMF USA* | **#SMFUSION**