Introduction to the NIST SP 800-171 Framework

March 22, 2018

Richard Collins & Chris Heitkamp
Clark Schaefer Consulting

clark schaefer consulting

Questions

How to ask a question during today's webinar?

- Use the "Chat" or "Question" feature on the GoToWebinar panel.
- You can also email Sara O'Banion at sobanion@clarkschaefer.com.
- Questions will be addressed at the end of the webinar.

Interested in CPE for today's event?

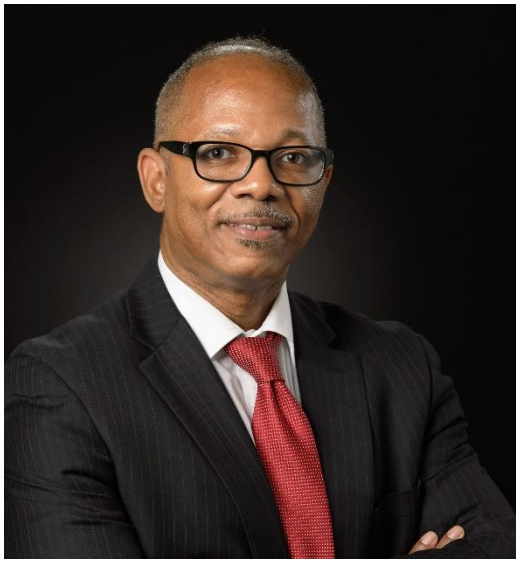
CPE Option 1 (Digital method)

- Be logged into the webinar for at least 50 min.
- Complete three of our interactive polls
- Complete the webinar survey

CPE Option 2 (Paper method)

- Be logged into the webinar for at least 50 min.
- Record the three CPE codes on the CPE form (located in the Handout List)
- Complete the webinar survey
- Send completed CPE form to nboudreau@clarkschaefer.com

Today's Presenters



Richard Collins

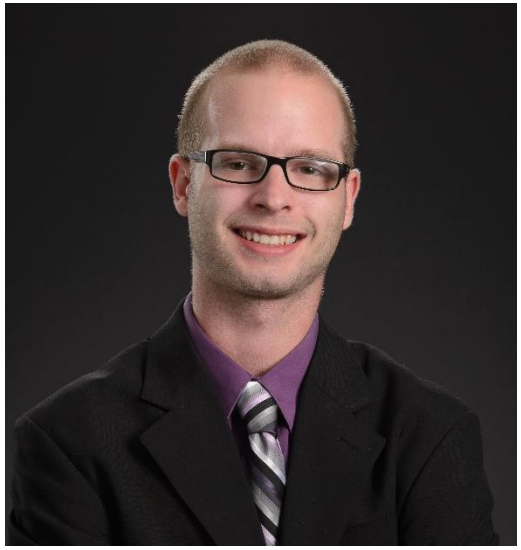
Sr. Consultant, Columbus Office

Connect on LinkedIn

Chris Heitkamp

Consultant, Cincinnati Office

Connect on LinkedIn



Introduction to the NIST 800-171 Framework:

Protecting Unclassified Information in Nonfederal Information Systems and Organizations

Richard Collins, Chris Heitkamp
March 22, 2018

clark schaefer consulting

Agenda

- What is NIST SP 800-171 and why was it created?
- What are the requirements for NIST 800-171?
- How to become compliant with NIST 800-171
- What are some of the challenges surrounding implementation of NIST 800-171

What is NIST SP 800-171 and why was it created?

clark schaefer consulting

Introduction

- On December 30, 2015, the U.S. Department of Defense (DOD) issued an interim rule to the Defense Federal Acquisition Regulation Supplement (DFARS) that gives directives to contractors to implement the requirements of the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171.
- These requirements protect the confidentiality of Controlled Unclassified Information (CUI) in non-federal systems and organizations. Contractors and subcontractors in many cases, were to establish these requirements **no later than December 31, 2017**.

What is NIST 800-171 and CUI ?

- NIST 800-171 is a framework that specifies how your information systems and policies need to be setup in order to protect Controlled Unclassified Information (CUI).

- It is a set of requirements that must be adequately fulfilled within 14 control families.

- CUI is an open and uniform program to manage all unclassified information within the executive branch that requires safeguarding and dissemination controls.

Why was NIST 800-171 created?

Established CUI Program

- On November 4, 2010, the President signed Executive Order (EO) 13556 establishing the Controlled Unclassified Information (CUI) program.

Why was NIST 800-171 created?

Executive Departments and agencies applied their own adhoc policies & markings to unclassified information that requires safeguarding or dissemination controls resulting in:

Inefficient patchwork with more than 100 different policies and markings across the Executive branch	Unclear or unnecessary restrictive dissemination policies	Impediments to authorized information sharing

Why was NIST 800-171 created?

- EO 13556 called for a review of the categories, subcategories, and markings currently used by agencies to control unclassified information.
- EO 13556 established an Executive Agent, the National Archives & Records Administration, to manage the CUI process.
- Agencies submitted to the Executive Agent what CUI they were protecting and the basis for that protection.
- CUI Registry was published.

Why was NIST 800-171 created?

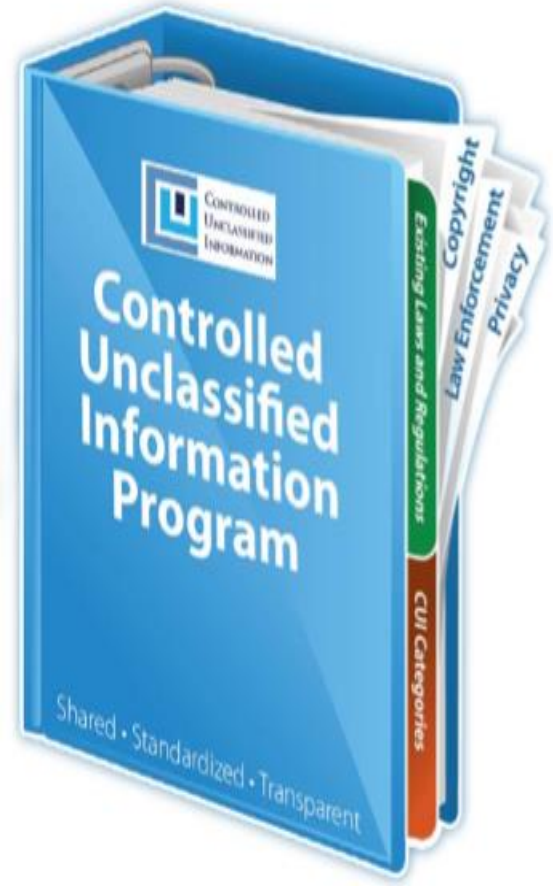
- Controlled Unclassified Information (CUI) replaces categories such as:
  - For Official Use Only (FOUO)
  - Sensitive But Unclassified (SBU)
  - Law Enforcement Sensitive (LES)

- Controlled Unclassified Information (CUI) versus Freedom of Information Act (FOIA). CUI does not prohibit a request for FOIA.

Why was NIST 800-171 created?

One, Uniformed, shared and transparent system for safeguarding and disseminating CUI that:

Establishes common understanding of CUI control	Promotes Information Sharing	Reinforces existing regulations and FOIA exemptions



Covered Defense Information (CDI)

NIST 800-171 also requires anyone accessing Covered Defense Information (CDI) to toughen their cyber security standards.

What is CDI?

Covered Defense Information (CDI)

- CDI means unclassified controlled technical information or other information that requires safeguarding or dissemination controls.
- The scope of NIST 800-171 is limited to systems that store CDI;
- And/or, information which the contractor accumulates in support of the contract. This expansive requirement and will have a dramatic impact on the number of systems that must be considered in-scope of a gap assessment.

Covered Defense Information's (CDIs) Four (4) Categories

1. • *Covered Technical Information ("CTI")*
2. • *Operations Security*
3. • *Export Controlled Information*
4. • *Any Other Information*

NIST SP 800-171 Requirements

clark schaefer consulting

Basic Requirements

Basic Security Requirements:

- Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

- Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Derived Requirements

Derived Security Requirements:

- Track, review, approve/disapprove, and audit changes to information systems.

- Analyze the security impact of changes prior to implementation.

NIST SP 800-171 requirements

- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations,
  - Framework to heighten security of information systems
  - Revision 5
- Federal Information Processing Standard (FIPS) Publication 200
  - Minimum Security Requirements for Federal Information and Information Systems
- 14 Control Families

NIST SP 800-171: Control Families

Access Control (3.1)

Awareness & Training (3.2)

Audit & Accountability (3.3)

Configuration Management (3.4)

Identification & Authentication (3.5)

NIST SP 800-171: Control Families

Incident Response (3.6)

Maintenance (3.7)

Media Protection (3.8)

Personnel Security (3.9)

Physical Protection (3.10)

NIST SP 800-171: Control Families

Risk Assessment (3.11)

Security Assessment (3.12)

Systems & Communications Protection (3.13)

Systems & Information Integrity (3.14)

Control Family Example

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.11 RISK ASSESSMENT				
Basic Security Requirements				
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	RA-3	Risk Assessment	A.12.6.1*	Management of technical vulnerabilities
Derived Security Requirements				
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities
	RA-5(5)	Vulnerability Scanning *Privileged Access*	*No direct mapping.*	
3.11.3 Remediate vulnerabilities in accordance with risk assessments.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities

Control Terms

- While mapping controls for NIST SP 800-171 a few terms to note are:
  - NCO
  - FED
  - NFO
  - CUI
- These terms are utilized in determining how the implementation of each control is handled.

Who could NIST 800-171 effect?

- Individuals with system development life cycle responsibilities
- Individuals with acquisition or procurement responsibilities
- Individuals with system, security, or risk management and oversight responsibilities; and
- Individuals with security assessment and monitoring responsibilities

Who could NIST SP 800-171 effect?

- Roles
  - CIO/CISO
  - Director of IT
  - Security Officers
  - Legal
  - Compliance
- Firms
  - Department of Defense Contractors
  - Implementation across multiple industries

NIST SP 800-171 Utilization

- NIST SP 800-171 became a requirement for Department of Defense contractors as a way for the government to impose stricter regulations on CUI, but other industries are beginning to look at the framework as a requirement as well.

- Any firm could use the framework to help better their security practices even if they do not have compliance obligations.

- The Department of Education has been looking at making NIST SP 800-171 a regulatory requirement for universities to help protect data.

Implementation of NIST SP 800-171

clark schaefer consulting

Where Do I Start? How Do I Comply with NIST SP 800-171?

1. Perform a Gap Analysis
2. Determine where do you process CDI and CUI?
3. Assess whether you are FEDRAMP Certified?
4. Establish an Incident Response Plan
5. Implement Changes to be Compliant

What Happens If A Contractor Missed the December 31, 2017 Deadline?

- It's a Defense Federal Acquisition Regulation (DFAR) requirement.

- A non-compliant contract with the U.S. Government could lead to…

- Contract Termination
- Criminal Fraud Charges
- Breach of Contract Lawsuits

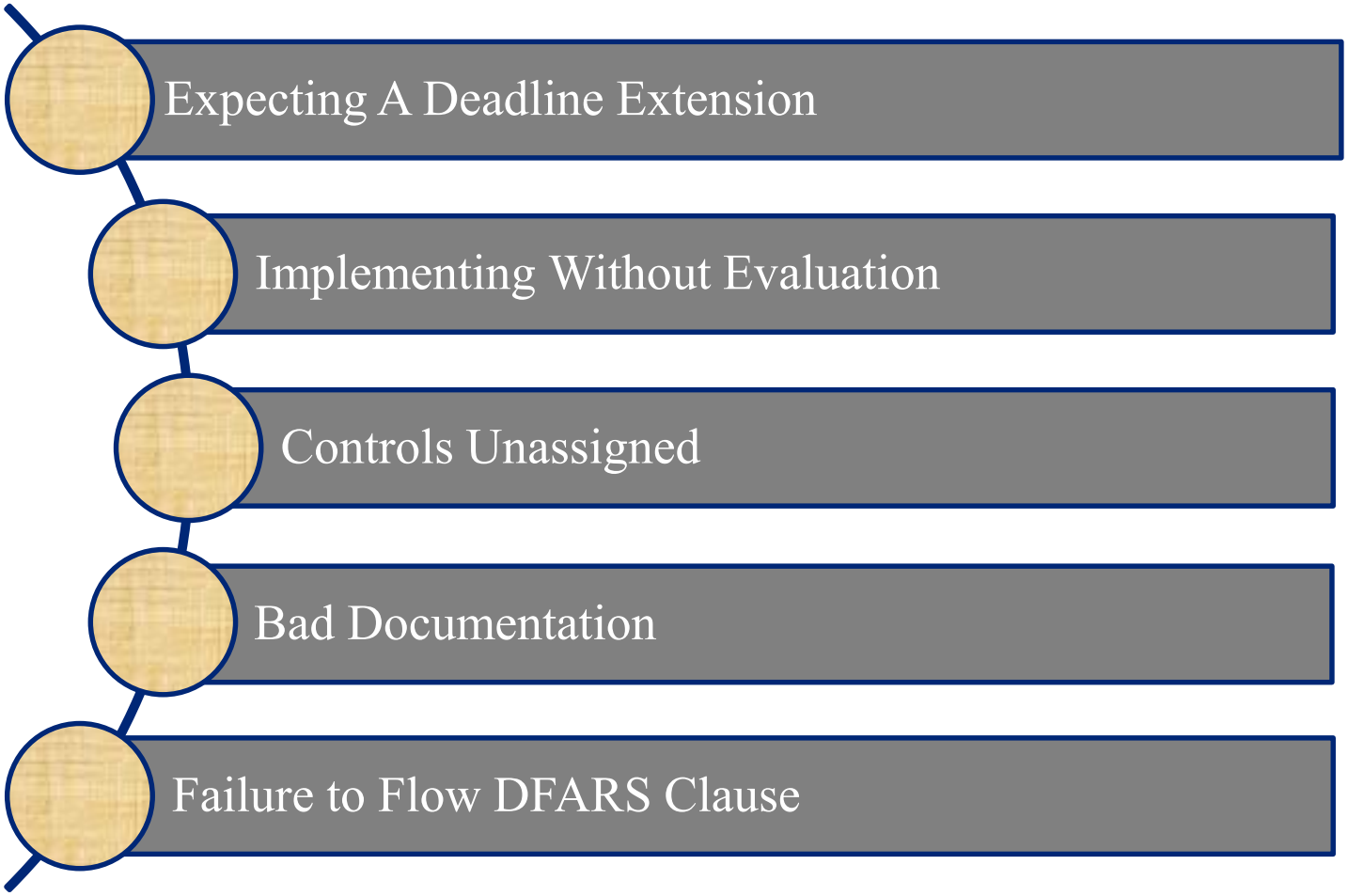
Registration Requirements

- After successfully implementing NIST SP 800-171 all contractors containing CUI are required to register with the Department of Defense by purchasing a security certificate to report data breaches in a timely manner

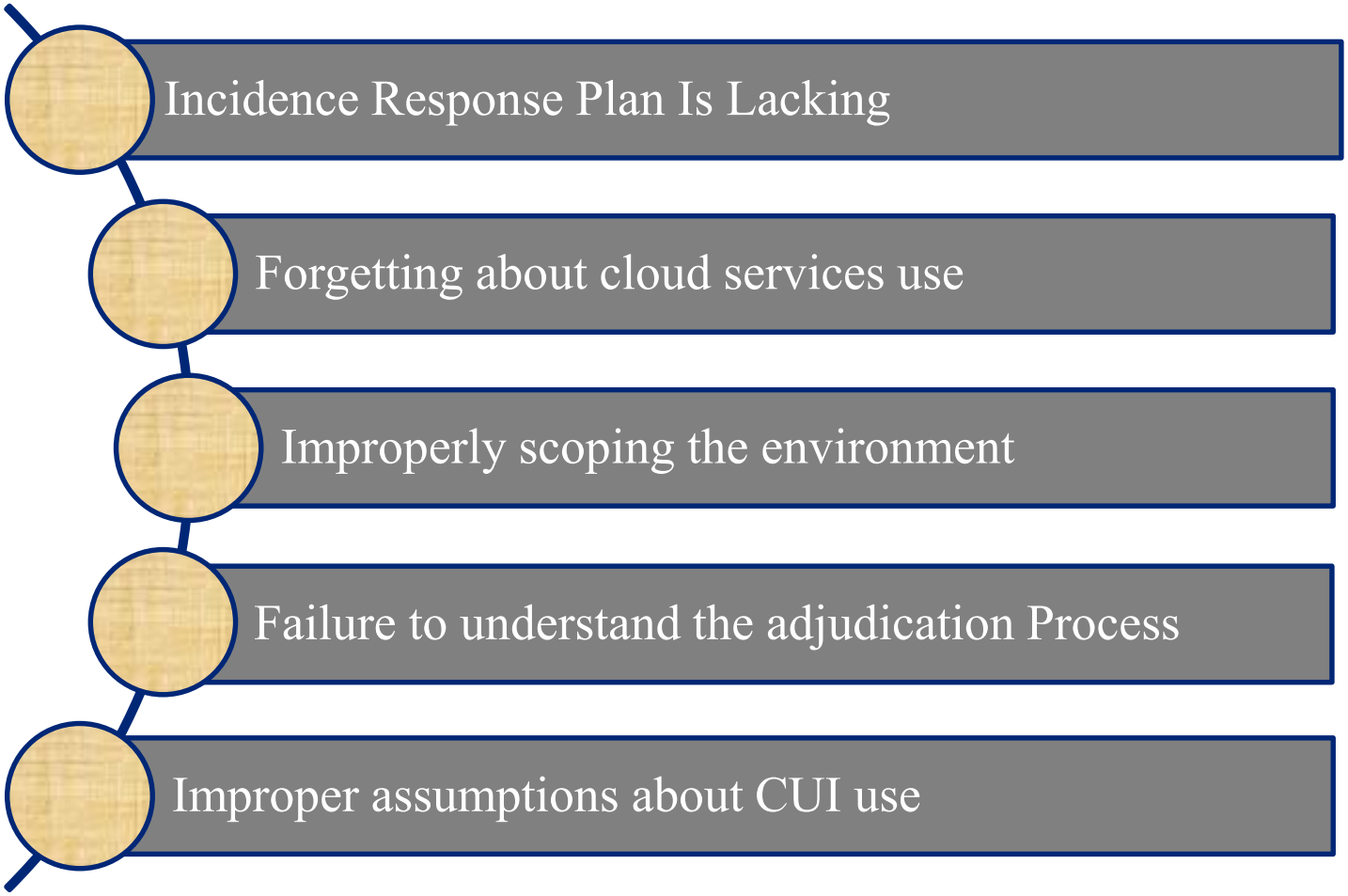
- An organization can purchase the security certificate through a DoD verified vendor such as IdenTrust at https://identrust.com/nist-800-171/index.html.

- Should a data breach occur, an organization must report it to the DoD through their website at https://dibnet.dod.mil/portal/intranet/Splashpage where the security certificate they purchased will allow access

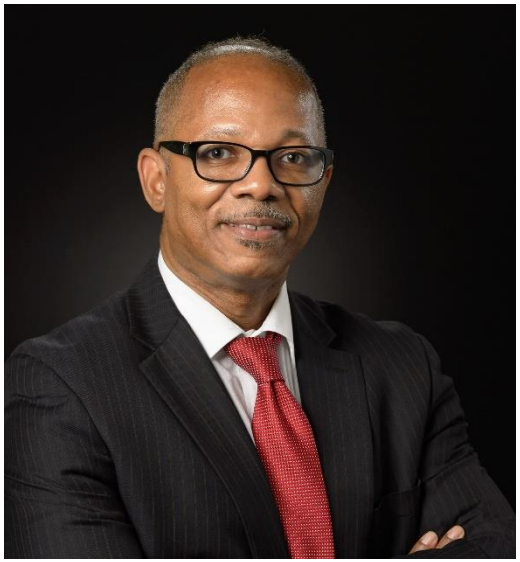
The Top 10 Issues in Implementing NIST SP 800-171 Requirements



The Top 10 Issues in Implementing NIST SP 800-171 Requirements



Questions?

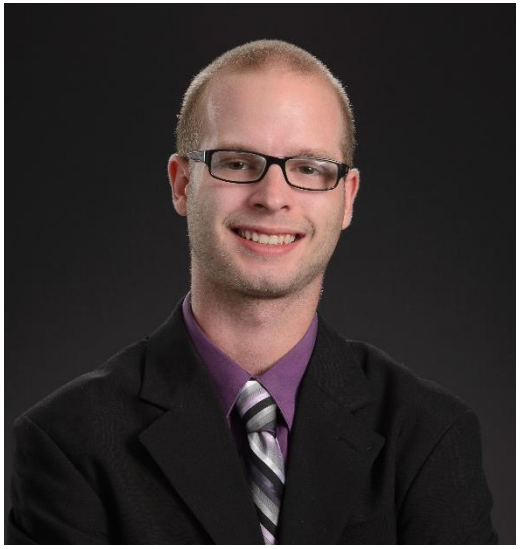


Richard Collins

Sr. Consultant, Columbus Office

rcollins@clarkschaefer.com

Connect on LinkedIn



Chris Heitkamp

Consultant, Cincinnati Office

cheitkamp@clarkschaefer.com

Connect on LinkedIn

CPE Overview

CPE Option 1 (Digital method)

- Be logged into the webinar for at least 50 min.
- Complete three of our interactive polls
- Complete the webinar survey

CPE Option 2 (Paper method)

- Be logged into the webinar for at least 50 min.
- Record the three CPE codes on the CPE form (located in the Handout List)
- Complete the webinar survey
- Send completed CPE form to nboudreau@clarkschaefer.com