Reading Between the Lines:

Leveraging the Assumptions Behind CMMC to Save Time, Money, & Your Sanity

Jacob Horne
DefCERT

March 4th, 2021

DEFCERT

Goals

Understand the Origins of Technical Debt

Assumptions They Make

Assumptions You Make

DEFCERT

“Your assumptions are your windows on the world. Scrub them off every once in a while, or the light won't come in.”

- Isaac Asimov

DEFCERT

May 27, 2009

the WHITE HOUSE
PRESIDENT BARACK OBAMA

BRIEFING ROOM | ISSUES | THE ADMINISTRATION | 1600 PENN

HOME · BRIEFING ROOM · PRESIDENTIAL ACTIONS · PRESIDENTIAL MEMORANDA

Briefing Room

- Your Weekly Address
- Speeches & Remarks
- Press Briefings
- Statements & Releases
- White House Schedule
- Presidential Actions
  - Executive Orders
  - **Presidential Memoranda**
  - Proclamations
- Legislation
- Nominations & Appointments
- Disclosures

The White House

May 27, 2009

Presidential Memorandum- Classified Information and Controlled Unclassified Information

THE WHITE HOUSE
Office of the Press Secretary

For Immediate Release May 27, 2009

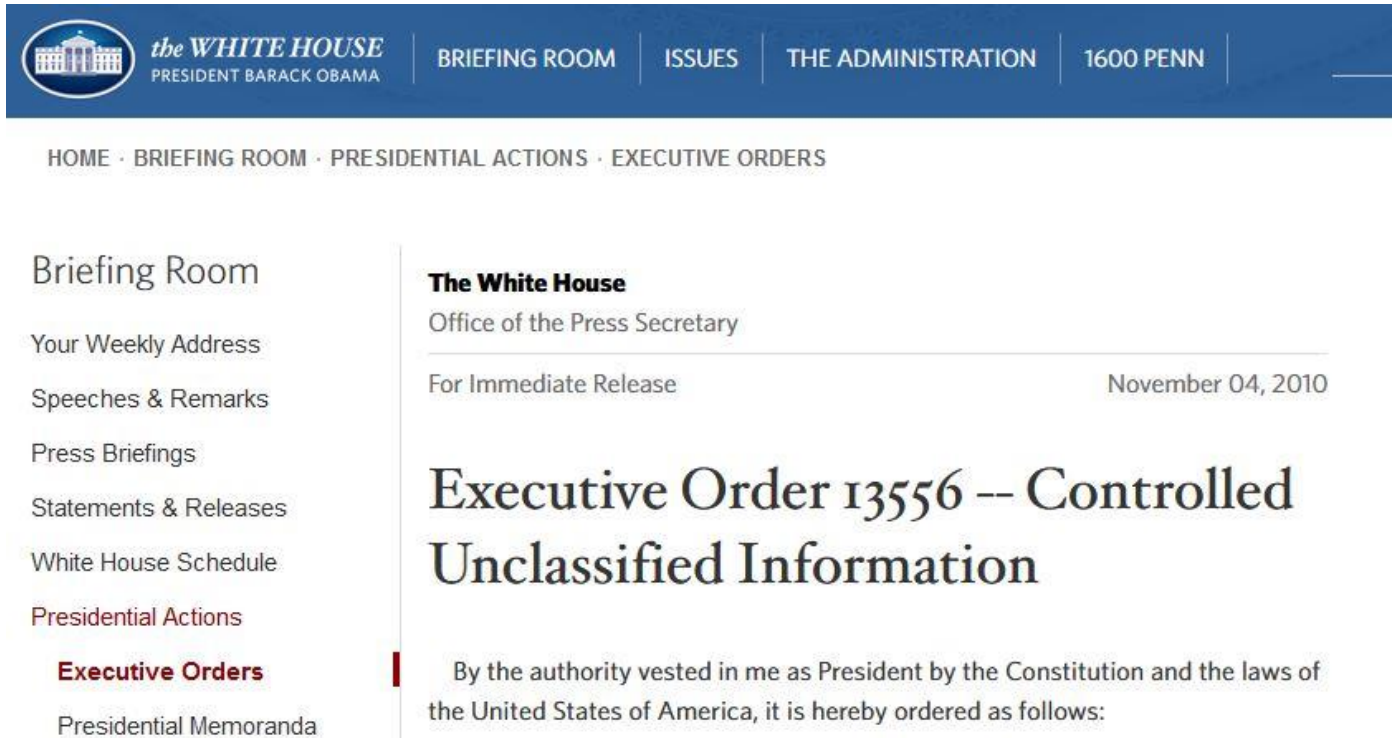
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Classified Information and Controlled Unclassified Information

DEFCERT

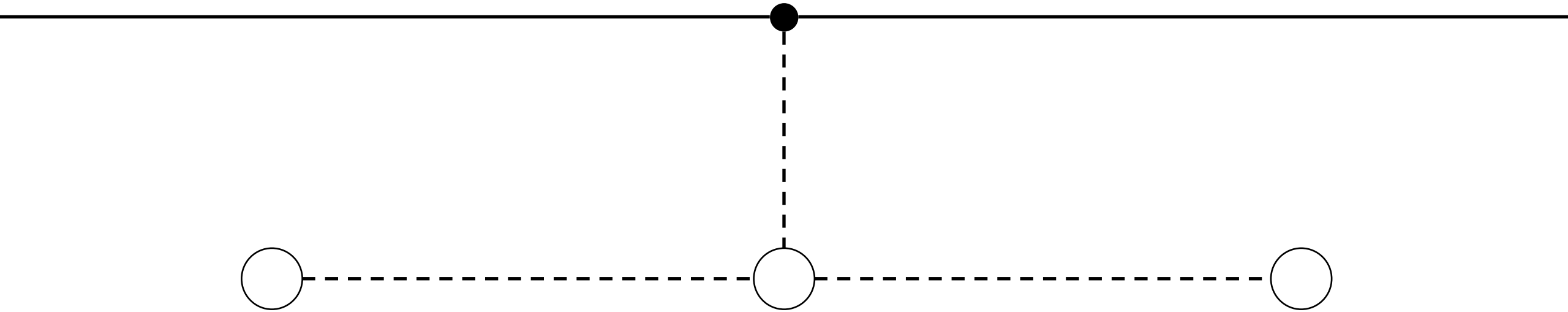
August 25, 2009

November 04, 2010



DEFCERT

November 04, 2010



Federal CUI Rule Implementing the EO

Federal Acquisition Regulation (FAR) for CUI

Security Requirements for Non-Federal Systems

DEFCERT

A Timeline of Assumptions

Mar 2010

DFARS "RFC"
DFARS Case
2008-D028

Nov 2010

Feb 2021

E.O. 14017

DEFCERT

March 03, 2010

<u>The DFARS did not address</u>:

- The safeguarding of unclassified DoD information within industry.
- Cyber intrusion reporting for that information.

<u>Purpose</u>:

- Implement adequate security measures to safeguard DoD information on unclassified industry information systems from unauthorized access and disclosure.
- Prescribe reporting to the Government with regard to certain cyber intrusion events that affect DoD information resident or transiting on contractor unclassified information systems.

Safeguarding Unclassified Information

DFARS Case 2008-D028: RFC

March 03, 2010

DFARS 252.204-7XXX

Basic Safeguarding of Unclassified Information Within Industry

DFARS 252.204-7YYY

Enhanced Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry

Relevant Information Types

- Critical Program Information
- ITAR and EAR
- Withheld from FOIA
- Controlled Access/Dissemination Designations (FOUO, SBU, LD, Proprietary, OC, LES, etc.)
- DoD Distribution Statements
- Withheld Unclassified Technical Data
- PII

DEFCERT

A Timeline of Assumptions

Mar 2010

DFARS "RFC"
DFARS Case
2008-D028

Jun 2011

Proposed Rule
DFARS Case
2011-D039

Nov 2010

Feb 2021

E.O. 14017

DEFCERT

June 28, 2011

Objective:

- Avoid compromise of unclassified computer networks on which DoD information is resident on or transiting through contractor information systems.

- Prevent the exfiltration of DoD information on such systems.

Safeguarding Unclassified DoD Information

DFARS Case 2011-D039: Proposed Rule

June 28, 2011

DFARS 252.204-7XXX

Basic Safeguarding of Unclassified Information Within Industry

- Protecting unclassified Government information on public computers or websites
- Transmitting electronic information
- Transmitting voice and fax information
- Physical or electronic barriers
- Sanitization
- Intrusion protection
- Transfer limitations

DFARS 252.204-7YYY

Enhanced Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry

- 59 controls from NIST SP 800-53

"Adequate Security"

Protective measures are applied commensurate with the risks (i.e., consequences and their probability) of loss, misuse, or unauthorized access to or modification of information.

DEFCERT

Safeguarding Unclassified DoD Information

DFARS Case 2011-D039: Proposed Rule

June 28, 2011

DFARS 252.204-7XXX

Basic Safeguarding of Unclassified Information Within Industry

- Basic protection are routine business.

DFARS 252.204-7YYY

Enhanced Safeguarding and Cyber Intrusion Reporting of Unclassified DoD Information Within Industry

- Some unclassified DoD data requires special handling and reporting.

“Reasonable Rule of Thumb”

Small business security budget:
0.5% of total revenues

DEFCERT

A Timeline of Assumptions

Mar 2010

DFARS "RFC"
DFARS Case
2008-D028

Jun 2011

Proposed Rule
DFARS Case
2011-D039

Nov 2010

Aug 2012

Proposed Rule
FAR Case 2011-020

Feb 2021

E.O. 14017

August 24, 2012

The FAR did not address:

- The safeguarding of contractor information systems that contain or process information provided by or generated for the Government (other than public information).

Objective:

- Improve the protection of information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems by employing basic security measures, as identified in the clause to appropriately protect information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems from unauthorized disclosure, loss, or compromise.

Basic Safeguarding of Contractor Information Systems

FAR Case 2011-020: Proposed Rule

August 24, 2012

FAR 52.204-XX

Basic Safeguarding of Unclassified Information Within Industry

Requires the contractor to provide protective measures to information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems in the following areas:

- Public computers or Web sites.
- Transmitting electronic information.
- Transmitting voice and fax information.
- Physical and electronic barriers.
- Sanitization.
- Intrusion protection.
- Transfer limitations

> "The resultant cost impact is considered not significant, since the first-level protective measures (i.e., updated virus protection, the latest security software patches, etc.) are typically employed as part of the routine course of doing business."

> "This proposed rule applies to all Federal contractors and appropriate subcontractors regardless of size or business ownership."

DEFCERT

A Timeline of Assumptions

Mar 2010

DFARS "RFC"
DFARS Case
2008-D028

Jun 2011

Proposed Rule
DFARS Case
2011-D039

Nov 2013

Final Rule
DFARS Case
2011-D039

Nov 2010

Executive Order 13556 -- Controlled Unclassified Information

Aug 2012

Proposed Rule
FAR Case 2011-020

Feb 2021

Executive Order on America's Supply Chains

E.O. 14017

Safeguarding Unclassified Controlled Technical Information

DFARS Case 2011-D039: Final Rule

November 17, 2013

DFARS 252.204-7012

Safeguarding of Unclassified Controlled Technical Information

- Reduced scope of information covered.
- Information retention requirement: 90 days.
- 13 pieces of reportable information.
- No Federal CUI Policy for Agencies.
- No Federal CUI Policy for Industry.
- DoD has existing authority to protect CTI.

DEFCERT

November 17, 2013

DFARS 252.204-7012

Safeguarding of Unclassified Controlled Technical Information

- Increased costs accounted for through the normal course of business
- Costs are spread across multiple contracts
- Costs are allowable: chargeable to indirect cost pools.
- NIST SP 800-53 controls closely parallel mainstream ISO 27002, therefore costs are reasonable.

> "The contractor's size classification is not a sufficient reason to allow a contractor to fail to protect technical information as required by clause 252.204-7012."

> "The Government does not intend to directly pay for the operating costs associated with the rule."

DEFCERT

A Timeline of Assumptions

May 2015

Federal CUI Program
Proposed Rule – 32 CFR 2002

Mar 2010

DFARS "RFC"
DFARS Case
2008-D028

Jun 2011

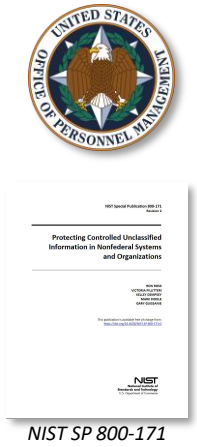
Proposed Rule
DFARS Case
2011-D039

Nov 2013

Final Rule
DFARS Case
2011-D039

Nov 2010

Jun 2015



NIST SP 800-171

Aug 2012

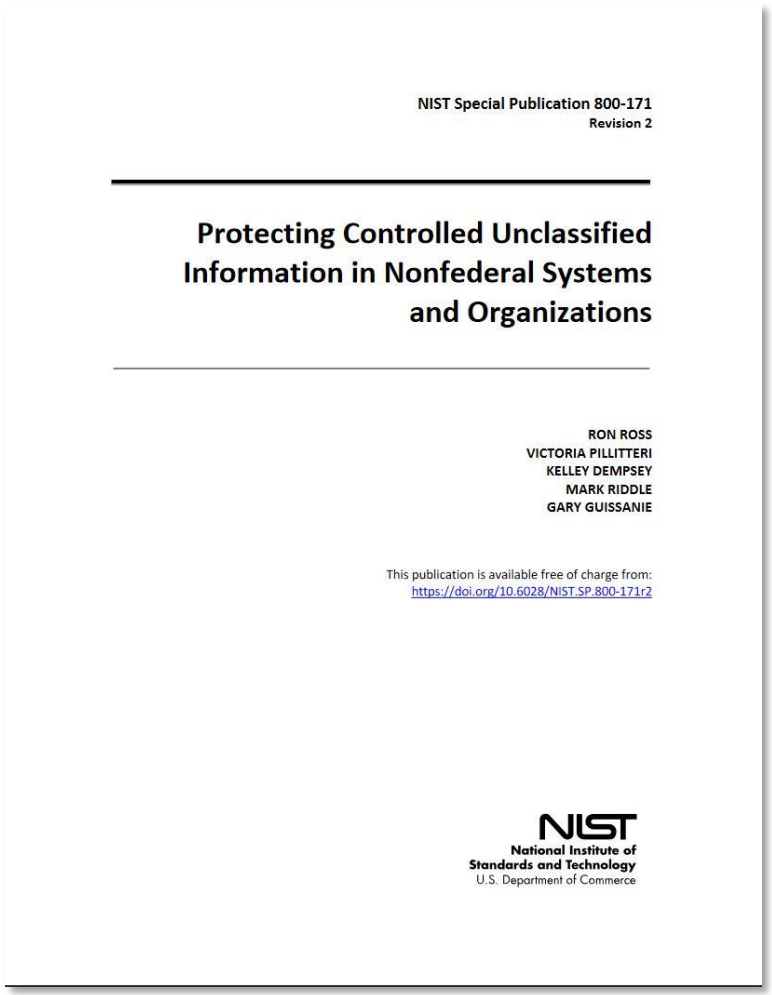
Proposed Rule
FAR Case 2011-020

Feb 2021

E.O. 14017

DEFCERT

June 2015



NIST Special Publication 800-171
Revision 2

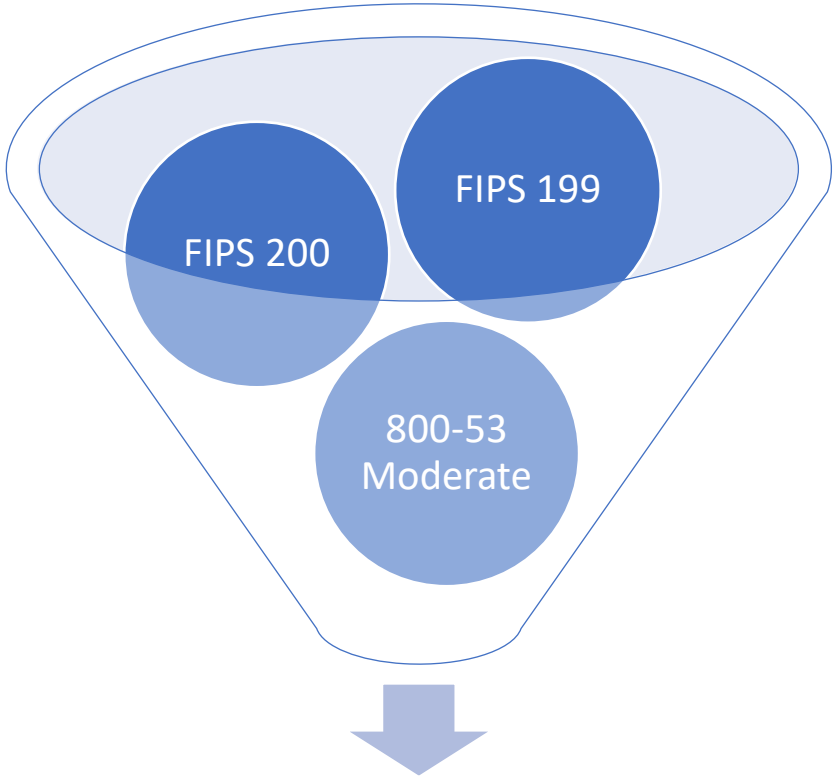
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Thousands of Controls



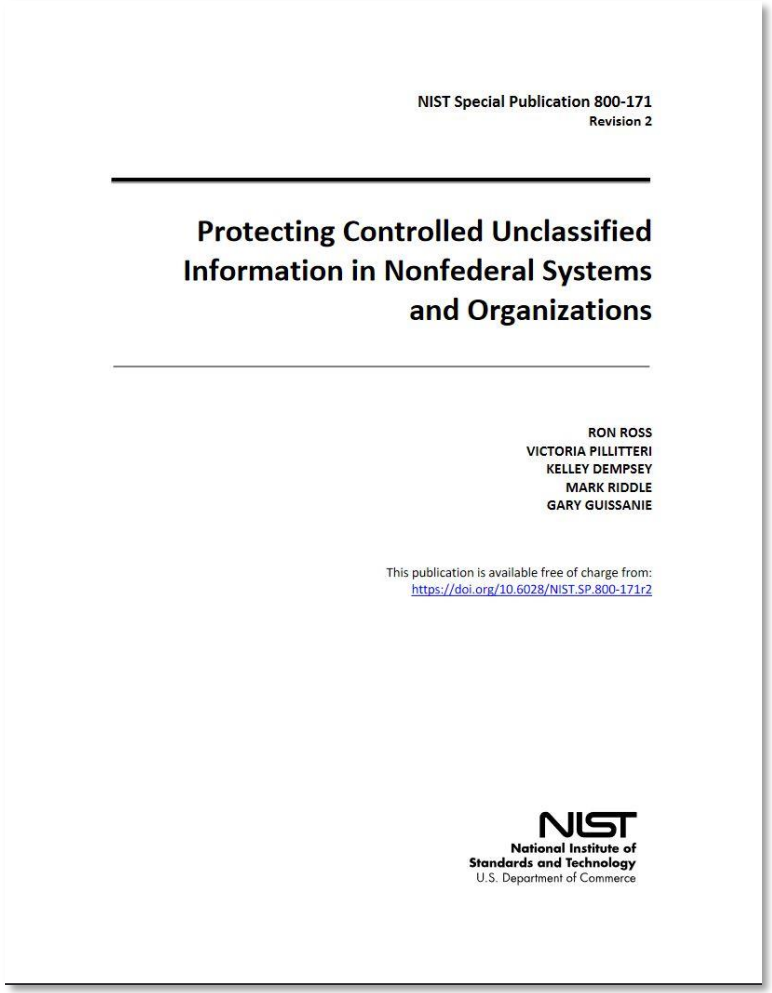
110 Requirements

DEFCERT

Protecting Controlled Unclassified Information in Nonfederal Systems & Organizations

NIST SP 800-171

June 2015



NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Assume: Nonfederal organizations are -

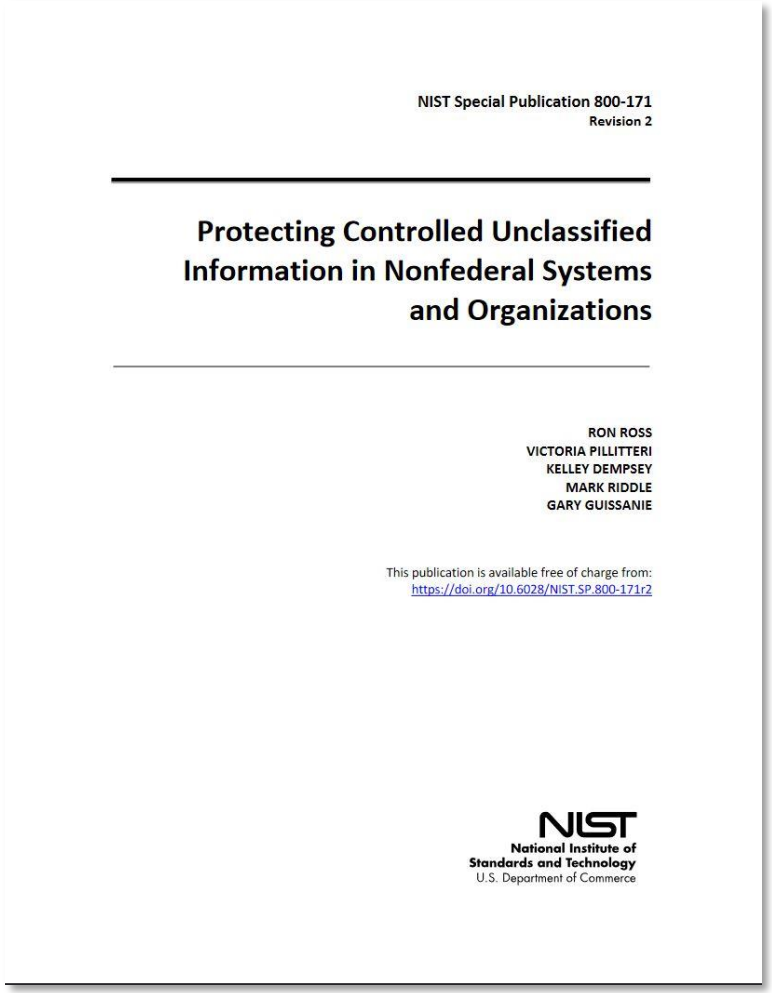
Not developing or acquiring systems specifically for the purpose of processing, storing, or transmitting CUI.

> *"Whatever we were going to do with regard to requirements, it would be relatively comfortable for those organizations in-line with what they're already doing to continue what they were already doing."*

- Dr. Ron Ross, NIST Fellow (2015)

DEFCERT

June 2015


NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Assume: Nonfederal organizations have -

Safeguarding measures in place to protect their information: may be sufficient to satisfy CUI requirements.

> *"We assume they have some level of protection in place. Whether they are using the NIST catalog of controls or using ISO 27000 or the new CSF – they're protecting their stuff because they have to in order to stay in business."*

> *"So, we already know that they are doing a lot and that was one of our tailoring criteria: we didn't want to tell them things that we already assumed they were doing."*

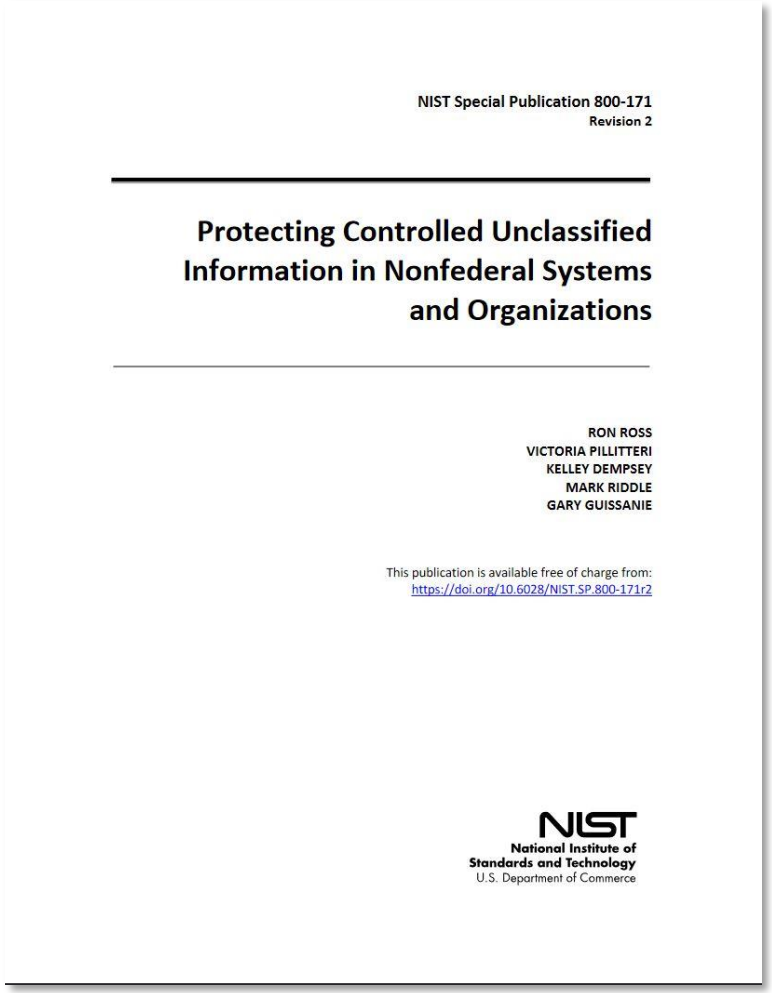
- Dr. Ron Ross, NIST Fellow (2015)

DEFCERT

Protecting Controlled Unclassified Information in Nonfederal Systems & Organizations

NIST SP 800-171

June 2015

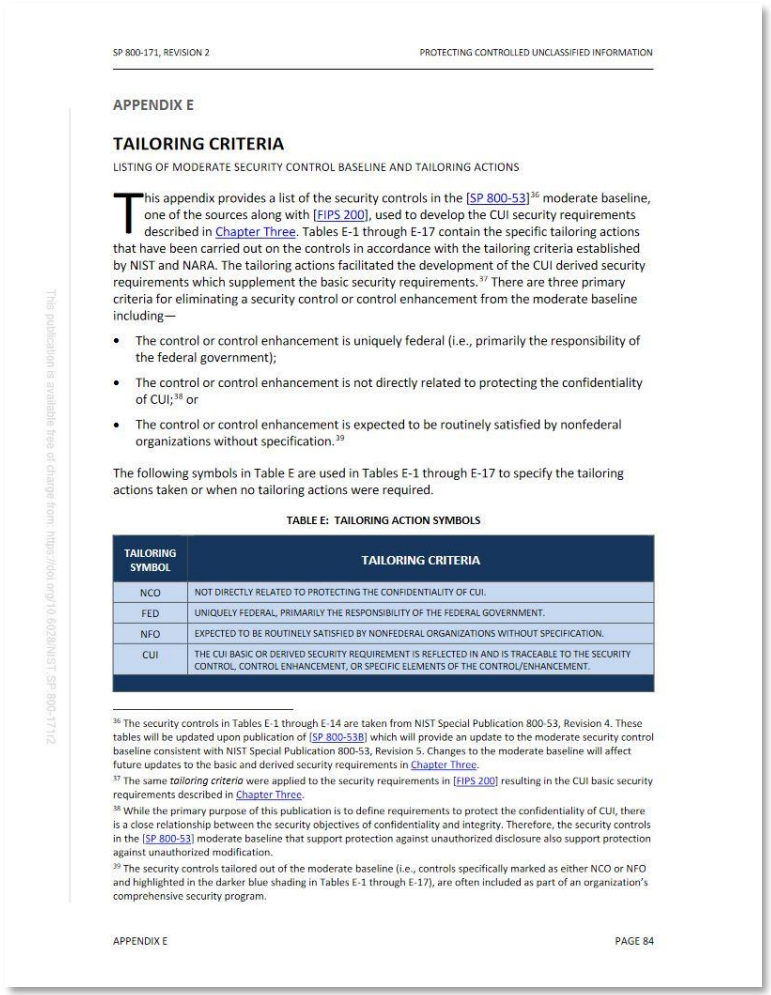


> *"Now, it could happen that some of our assumptions (the things that we thought they were doing – they may not be doing) but again, we had to make some design decisions on how these requirements came out."*

\- Dr. Ron Ross, NIST Fellow (2015)

DEFCERT

June 2015



SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

APPENDIX E

TAILORING CRITERIA

LISTING OF MODERATE SECURITY CONTROL BASELINE AND TAILORING ACTIONS

This appendix provides a list of the security controls in the [SP 800-53][36] moderate baseline, one of the sources along with [FIPS 200], used to develop the CUI security requirements described in Chapter Three. Tables E-1 through E-17 contain the specific tailoring actions that have been carried out on the controls in accordance with the tailoring criteria established by NIST and NARA. The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements.[37] There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government);
- The control or control enhancement is not directly related to protecting the confidentiality of CUI;[38] or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.[39]

The following symbols in Table E are used in Tables E-1 through E-17 to specify the tailoring actions taken or when no tailoring actions were required.

TABLE E: TAILORING ACTION SYMBOLS

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

[36] The security controls in Tables E-1 through E-14 are taken from NIST Special Publication 800-53, Revision 4. These tables will be updated upon publication of [SP 800-53B] which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements in Chapter Three.

[37] The same *tailoring criteria* were applied to the security requirements in [FIPS 200] resulting in the CUI basic security requirements described in Chapter Three.

[38] While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between the security objectives of confidentiality and integrity. Therefore, the security controls in the [SP 800-53] moderate baseline that support protection against unauthorized disclosure also support protection against unauthorized modification.

[39] The security controls tailored out of the moderate baseline (i.e., controls specifically marked as either NCO or NFO and highlighted in the darker blue shading in Tables E-1 through E-17), are often included as part of an organization's comprehensive security program.

APPENDIX E PAGE 84

62 “NFO” Controls

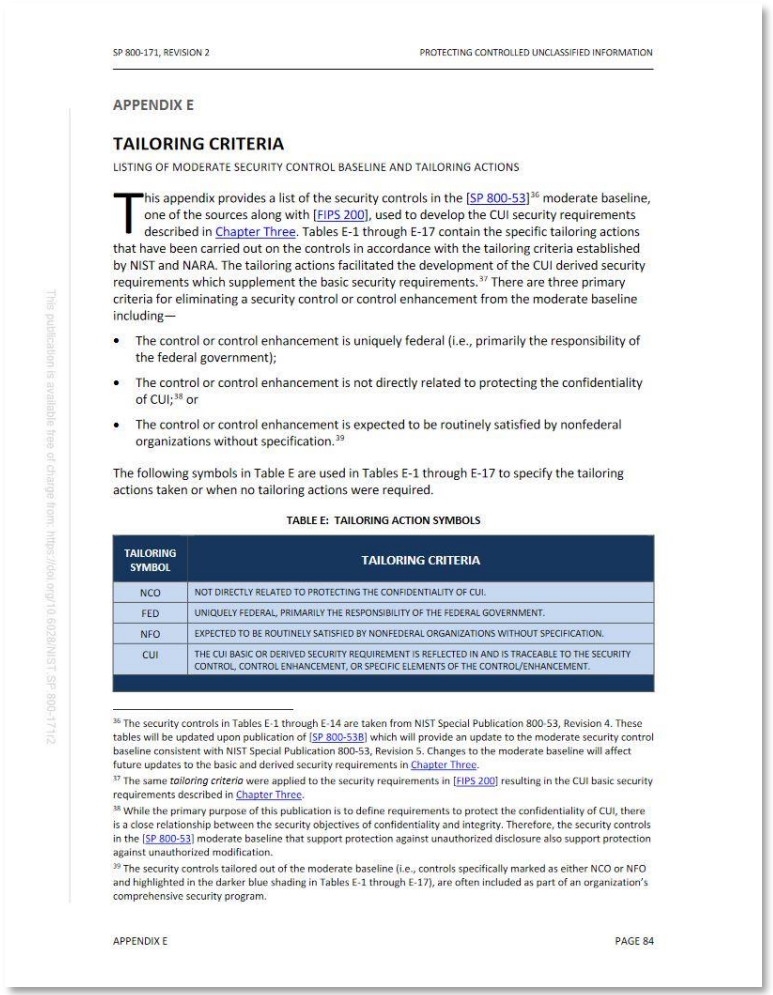
> *“We went through and took a hard look and said, ‘Do you think we have to tell people to do this? Or should that be kind of expected?’”*

> *“In the modern world of running information systems and having security programs – these requirements – we think that we don’t have to tell people to do them.”*

\- Dr. Ron Ross, NIST Fellow (2015)

DEFCERT

June 2015



SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

APPENDIX E

TAILORING CRITERIA

LISTING OF MODERATE SECURITY CONTROL BASELINE AND TAILORING ACTIONS

This appendix provides a list of the security controls in the [SP 800-53][36] moderate baseline, one of the sources along with [FIPS 200], used to develop the CUI security requirements described in Chapter Three. Tables E-1 through E-17 contain the specific tailoring actions that have been carried out on the controls in accordance with the tailoring criteria established by NIST and NARA. The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements.[37] There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government);
- The control or control enhancement is not directly related to protecting the confidentiality of CUI;[38] or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.[39]

The following symbols in Table E are used in Tables E-1 through E-17 to specify the tailoring actions taken or when no tailoring actions were required.

TABLE E: TAILORING ACTION SYMBOLS

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

[36] The security controls in Tables E-1 through E-14 are taken from NIST Special Publication 800-53, Revision 4. These tables will be updated upon publication of [SP 800-53B] which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements in Chapter Three.

[37] The same *tailoring criteria* were applied to the security requirements in [FIPS 200] resulting in the CUI basic security requirements described in Chapter Three.

[38] While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between the security objectives of confidentiality and integrity. Therefore, the security controls in the [SP 800-53] moderate baseline that support protection against unauthorized disclosure also support protection against unauthorized modification.

[39] The security controls tailored out of the moderate baseline (i.e., controls specifically marked as either NCO or NFO and highlighted in the darker blue shading in Tables E-1 through E-17), are often included as part of an organization's comprehensive security program.

APPENDIX E PAGE 84

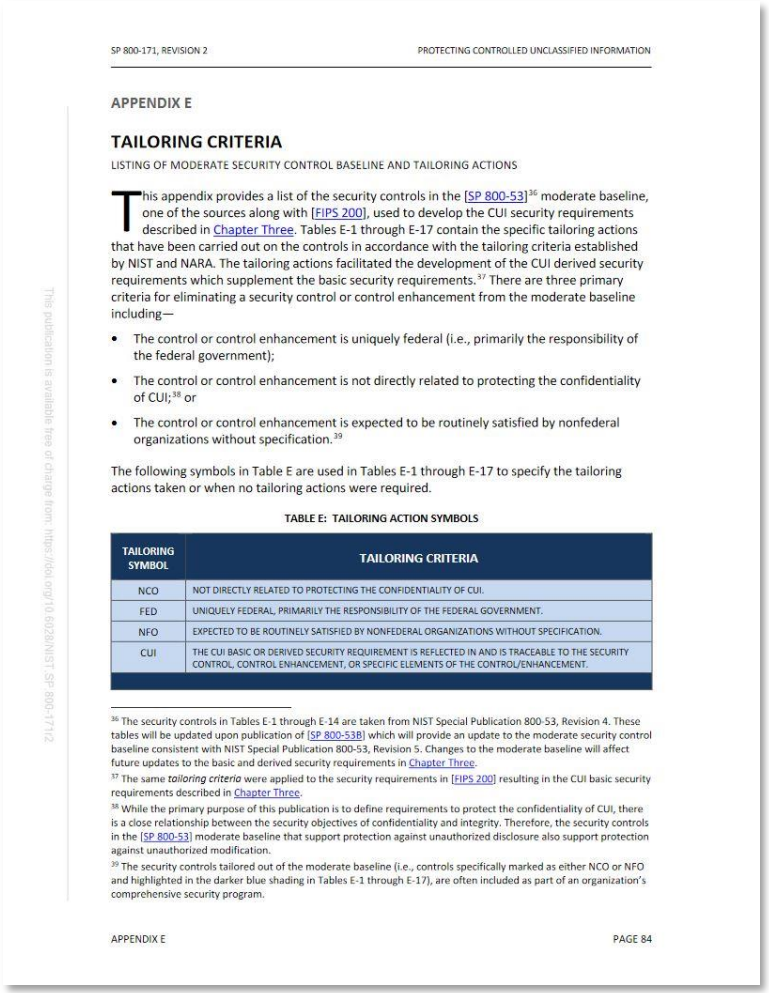
62 “NFO” Controls

> *“Got rid of all of the “-1 controls”. The first control. The policy and procedures control. We took those out because we assumed that organizations that are complying would most likely have policies and procedures.* ***That was not something that we wanted to tell them to do.***

- Dr. Ron Ross, NIST Fellow (2015)

DEFCERT

June 2015



SP 800-171, REVISION 2 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

APPENDIX E

TAILORING CRITERIA

LISTING OF MODERATE SECURITY CONTROL BASELINE AND TAILORING ACTIONS

This appendix provides a list of the security controls in the [SP 800-53][36] moderate baseline, one of the sources along with [FIPS 200], used to develop the CUI security requirements described in Chapter Three. Tables E-1 through E-17 contain the specific tailoring actions that have been carried out on the controls in accordance with the tailoring criteria established by NIST and NARA. The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements.[37] There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government);
- The control or control enhancement is not directly related to protecting the confidentiality of CUI;[38] or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.[39]

The following symbols in Table E are used in Tables E-1 through E-17 to specify the tailoring actions taken or when no tailoring actions were required.

TABLE E: TAILORING ACTION SYMBOLS

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

[36] The security controls in Tables E-1 through E-14 are taken from NIST Special Publication 800-53, Revision 4. These tables will be updated upon publication of [SP 800-53B] which will provide an update to the moderate security control baseline consistent with NIST Special Publication 800-53, Revision 5. Changes to the moderate baseline will affect future updates to the basic and derived security requirements in Chapter Three.

[37] The same *tailoring criteria* were applied to the security requirements in [FIPS 200] resulting in the CUI basic security requirements described in Chapter Three.

[38] While the primary purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between the security objectives of confidentiality and integrity. Therefore, the security controls in the [SP 800-53] moderate baseline that support protection against unauthorized disclosure also support protection against unauthorized modification.

[39] The security controls tailored out of the moderate baseline (i.e., controls specifically marked as either NCO or NFO and highlighted in the darker blue shading in Tables E-1 through E-17), are often included as part of an organization's comprehensive security program.

APPENDIX E PAGE 84

62 “NFO” Controls

SA – 9 *External Information System Services*

a. Require that providers of external system services comply with organizational security and privacy requirements…

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services…

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis…

DEFCERT

A Timeline of Assumptions

May 2015

Federal CUI Program
Proposed Rule – 32 CFR 2002

Mar 2010 — *DFARS "RFC"* DFARS Case 2008-D028

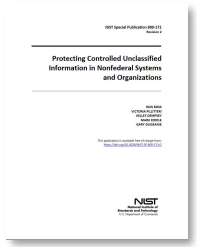
Jun 2011 — *Proposed Rule* DFARS Case 2011-D039

Nov 2013 — *Final Rule* DFARS Case 2011-D039

Aug 2015 — *Interim Rule* DFARS Case 2011-D018

Nov 2010

Jun 2015



NIST SP 800-171

Feb 2021

E.O. 14017

Aug 2012

Proposed Rule
FAR Case 2011-020

July 2015

FAR CUI Rule
OMB "RFC"

DEFCERT

August 25, 2015

Objective:

- Improve information security for DoD information stored on or transiting contractor systems as well as in a cloud environment.

- Urgent and compelling reasons exist to promulgate this interim rule…urgent need to protect covered defense information and gain awareness of the full scope of cyber incidents being committed against defense contractors.

- Recent high-profile breaches of Federal information show the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts

Network Penetration Testing & Contracting for Cloud Services

DFARS Case 2011-D018: Interim Rule

August 25, 2015

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

- Added to ensure that offerors are aware of the requirements of clause 252.204-7012

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

- Scope of the clause is expanded to cover the safeguarding of covered defense information and require contractors to report cyber incidents involving this new class of information

> "Of the required reporting fields several of them will likely require an information technology expert to provide information describing the cyber incident or at least to determine what information was affected, to be noted in the report."

DEFCERT

Network Penetration Testing & Contracting for Cloud Services

DFARS Case 2011-D018: Interim Rule

August 25, 2015

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

- Added to ensure that offerors are aware of the requirements of clause 252.204-7012

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

- Scope of the clause is expanded to cover the safeguarding of covered defense information and require contractors to report cyber incidents involving this new class of information

NIST SP 800-171 Replaces 800-53 Controls

Reduces required tasks by:

30%

DEFCERT

A Timeline of Assumptions

May 2015

Federal CUI Program
Proposed Rule – 32 CFR 2002

Mar 2010

DFARS "RFC"
DFARS Case
2008-D028

Jun 2011

Proposed Rule
DFARS Case
2011-D039

Nov 2013

Final Rule
DFARS Case
2011-D039

Aug 2015

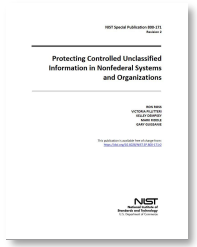
Interim Rule
DFARS Case
2011-D018

Dec 2015

Interim Rule
DFARS Case
2011-D018

Nov 2010

Jun 2015



NIST SP 800-171

Feb 2021

E.O. 14017

Aug 2012

Proposed Rule
FAR Case 2011-020

July 2015

FAR CUI Rule
OMB "RFC"

DEFCERT

Network Penetration Testing & Contracting for Cloud Services

DFARS Case 2011-D018: Interim Rule

December 29, 2015

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

Amending to provide additional time

Implementation Deadline:

Dec 31, 2017

DEFCERT

A Timeline of Assumptions

May 2015

Federal CUI Program
Proposed Rule – 32 CFR 2002

Mar 2010
DFARS "RFC"
DFARS Case
2008-D028

Jun 2011
Proposed Rule
DFARS Case
2011-D039

Nov 2013
Final Rule
DFARS Case
2011-D039

Aug 2015
Interim Rule
DFARS Case
2011-D018

Dec 2015
Interim Rule
DFARS Case
2011-D018

Oct 2016
Final Rule
DFARS Case
2011-D018

Nov 2010


Executive Order 13556 -- Controlled Unclassified Information

Jun 2015


Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST SP 800-171

Feb 2021


Executive Order on America's Supply Chains

E.O. 14017

Aug 2012

Proposed Rule
FAR Case 2011-020

July 2015

FAR CUI Rule
OMB "RFC"

DEFCERT

October 21, 2016

Objective:

- Improve information security for DoD information stored on or transiting contractor systems as well as in a cloud environment.

Network Penetration Testing & Contracting for Cloud Services

DFARS Case 2011-D018: Final Rule

October 21, 2016

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

- Added to ensure that offerors are aware of the requirements of clause 252.204-7012

"Implementing the minimum-security controls outlined in the DFARS clause may increase costs, protection of unclassified DoD information is deemed necessary."

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

- Cloud service providers that store, process, or transmit Covered Defense Information must meet FEDRAMP Moderate Equivalency.

"Implementation of the NIST SP 800-171 security requirements will provide significant benefit to the small business community in the form of increased protection of their intellectual property."

DEFCERT

October 21, 2016

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

> "The cost of compliance with the requirements of this rule is unknown as the cost is determined based on the make-up of the information system and the current state of security already in place."

October 21, 2016

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

"The security requirements in NIST SP 800-171 build upon the table of controls contained in the November 2013 version of DFARS clause 252.204-7012.

While there is additional effort for the difference, none of the effort to implement the original controls is lost."

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

"DoD does not develop "cost recovery models" for compliance with DFARS rules.

The requirements levied by this rule should be treated the same as those levied by any other new DFARS rule and the cost related to compliance should be considered during proposal preparation."

October 21, 2016

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

> "Cyber incident reporting, media preservation, and system access are not part of the contractor's adequate security obligations, but rather distinct requirements of the clause when a cyber incident occurs on a covered contractor information system."

October 21, 2016

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

Alternative Paths Considered for Small Entities:

- An exemption.
- Delaying for further costs analysis.
- Creating a different set of security requirements.

"Rejected as conflicting with the overarching purpose of this rule which is to increase the security of unclassified information that DoD has determined could result in harm if released."

"Regardless of the size of the contractor or subcontractor handling the information, the protection level of that information needs to be the same across the board."

DEFCERT

A Timeline of Assumptions

May 2015

Federal CUI Program
Proposed Rule – 32 CFR 2002

Mar 2010
DFARS "RFC"
DFARS Case
2008-D028

Jun 2011
Proposed Rule
DFARS Case
2011-D039

Nov 2013
Final Rule
DFARS Case
2011-D039

Aug 2015
Interim Rule
DFARS Case
2011-D018

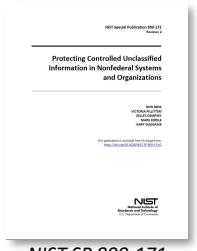
Dec 2015
Interim Rule
DFARS Case
2011-D018

Oct 2016
Final Rule
DFARS Case
2011-D018

Nov 2010


Executive Order 13556 -- Controlled Unclassified Information

Jun 2015


Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST SP 800-171

Feb 2021


Executive Order on America's Supply Chains

E.O. 14017

Aug 2012
Proposed Rule
FAR Case 2011-020

Jun 2016
Final Rule
FAR Case 2011-020

July 2015
FAR CUI Rule
OMB "RFC"

DEFCERT

June 15, 2016

FAR 52.204-21

Basic Safeguarding of Covered Contractor Information Systems

- Objective: of this rule is to require contractors to employ basic security measures, as identified in the clause, for any covered contractor information system.
- This final rule has basic safeguarding measures that are generally employed as part of the routine course of doing business.
- Provides for safeguarding the contractor information system, rather than specific information contained in the system.

> "This rule, which focuses on ensuring a basic level of safeguarding for any contractor system with Federal information, reflective of actions a prudent business-person would employ, is just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems."

A Timeline of Assumptions

May 2015
Federal CUI Program
Proposed Rule – 32 CFR 2002

Sep 2016
Federal CUI Program
Final Rule – 32 CFR 2002

Mar 2010
DFARS "RFC"
DFARS Case
2008-D028

Jun 2011
Proposed Rule
DFARS Case
2011-D039

Nov 2013
Final Rule
DFARS Case
2011-D039

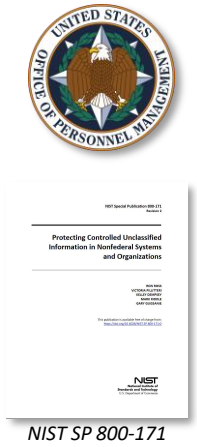
Aug 2015
Interim Rule
DFARS Case
2011-D018

Dec 2015
Interim Rule
DFARS Case
2011-D018

Oct 2016
Final Rule
DFARS Case
2011-D018

Nov 2010

Jun 2015



NIST SP 800-171

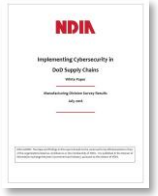
Jul 2017

E.O. 13806

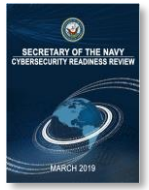
Jun 2018

SEADRAGON

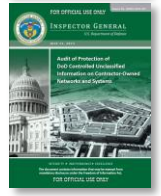
Summer 2018



Spring 2019



Summer 2019



Mar 2020

Feb 2021

E.O. 14017

Aug 2012
Proposed Rule
FAR Case 2011-020

Jun 2016
Final Rule
FAR Case 2011-020

July 2015
FAR CUI Rule
OMB "RFC"

DEFCERT

A Timeline of Assumptions

May 2015
Federal CUI Program
Proposed Rule – 32 CFR 2002

Sep 2016
Federal CUI Program
Final Rule – 32 CFR 2002

Mar 2010
DFARS "RFC"
DFARS Case
2008-D028

Jun 2011
Proposed Rule
DFARS Case
2011-D039

Nov 2013
Final Rule
DFARS Case
2011-D039

Aug 2015
Interim Rule
DFARS Case
2011-D018

Dec 2015
Interim Rule
DFARS Case
2011-D018

Oct 2016
Final Rule
DFARS Case
2011-D018

Nov 2010


Executive Order 13556 -- Controlled Unclassified Information

Jun 2015

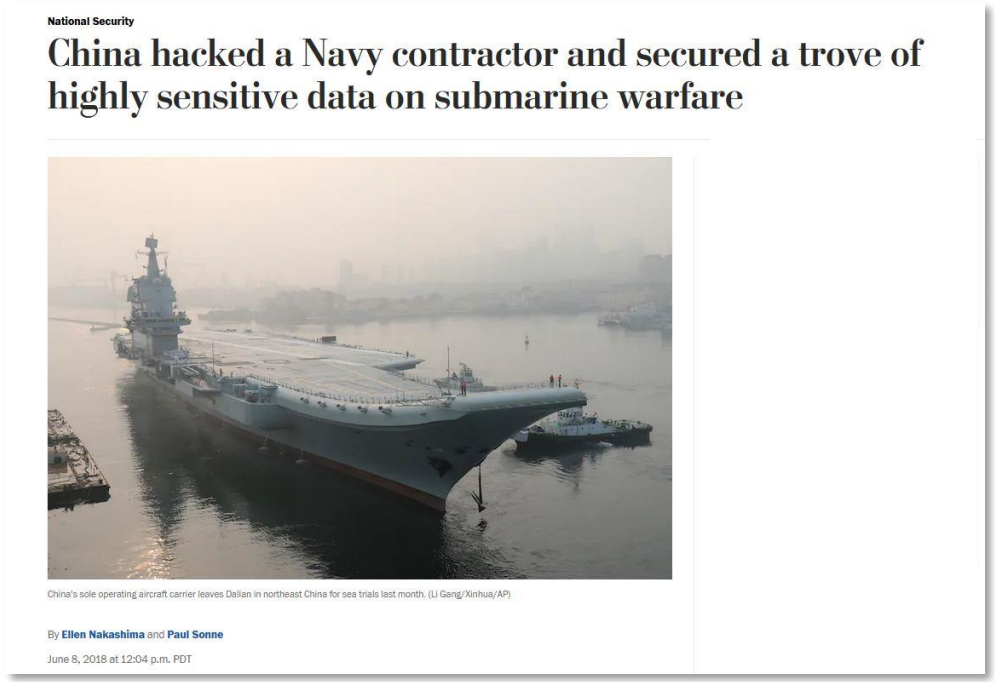
NIST SP 800-171

Jul 2017


E.O. 13806

Jun 2018

SEADRAGON


National Security

China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare

China's sole operating aircraft carrier leaves Dalian in northeast China for sea trials last month. (Li Gang/Xinhua/AP)

By Ellen Nakashima and Paul Sonne

June 8, 2018 at 12:04 p.m. PDT

Feb 2021


Executive Order on America's Supply Chains

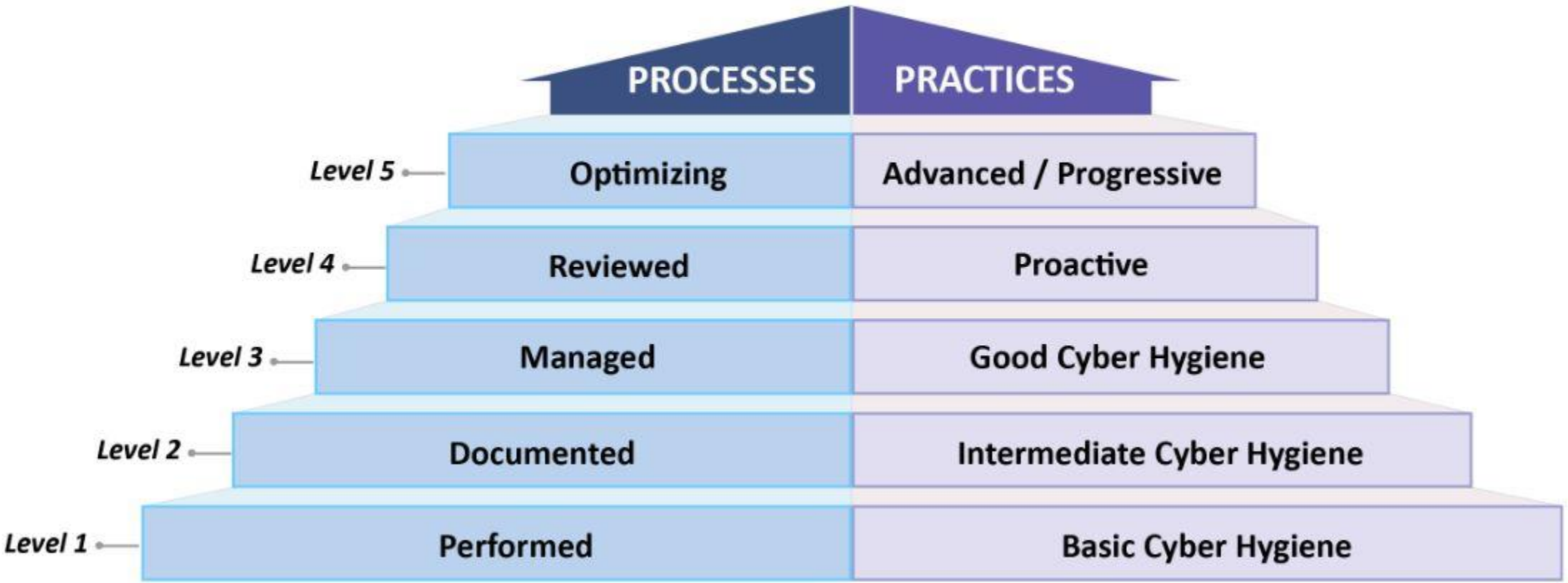
E.O. 14017

Aug 2012
Proposed Rule
FAR Case 2011-020

Jun 2016
Final Rule
FAR Case 2011-020

July 2015
FAR CUI Rule
OMB "RFC"

DEFCERT


PROCESSES
PRACTICES
Level 5
Optimizing
Advanced / Progressive
Level 4
Reviewed
Proactive
Level 3
Managed
Good Cyber Hygiene
Level 2
Documented
Intermediate Cyber Hygiene
Level 1
Performed
Basic Cyber Hygiene

Level 3

AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
AC.3.019	Terminate (automatically) user sessions after a defined condition.

CMMC Level 3

- **130 Requirements**
- **383 Practice Objectives**
- **323 Process Objectives**
- **706 Total**
- **50% - 70% Non-technical**

Level 3 AC Practices

Practices are presented in the order in which they appear in the *CMMC Model Matrix* from top to bottom, not numerical order.

AC.3.017

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] the duties of individuals requiring separation are defined;

[b] responsibilities for duties that require separation are assigned to separate individuals; and

[c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing divisions of responsibility and separation of duties; system security plan; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for defining divisions of responsibility and separation of duties; personnel with information security responsibilities; system or network administrators].

Test

[SELECT FROM: Mechanisms implementing separation of duties policy].

A Timeline of Assumptions

May 2015
Federal CUI Program
Proposed Rule – 32 CFR 2002

Sep 2016
Federal CUI Program
Final Rule – 32 CFR 2002

Mar 2010
DFARS "RFC"
DFARS Case
2008-D028

Jun 2011
Proposed Rule
DFARS Case
2011-D039

Nov 2013
Final Rule
DFARS Case
2011-D039

Aug 2015
Interim Rule
DFARS Case
2011-D018

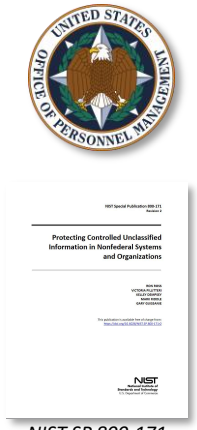
Dec 2015
Interim Rule
DFARS Case
2011-D018

Oct 2016
Final Rule
DFARS Case
2011-D018

Nov 2020
Interim Rule
DFARS Case
2019-D041

Nov 2010

Jun 2015



NIST SP 800-171

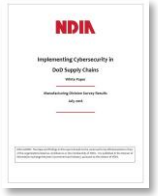
Jul 2017

E.O. 13806

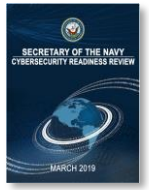
Jun 2018

SEADRAGON

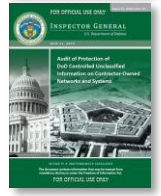
Summer 2018



Spring 2019



Summer 2019



Mar 2020

Feb 2021

E.O. 14017

Aug 2012
Proposed Rule
FAR Case 2011-020

Jun 2016
Final Rule
FAR Case 2011-020

July 2015
FAR CUI Rule
OMB "RFC"

DEFCERT

November 30, 2020

Objective: Provide the Department with:

- The ability to assess contractor implementation of NIST SP 800-171 security requirements.
- Assurances that DIB contractors can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flowed down to subcontractors in a multi-tier supply chain.

Neither the FAR clause, nor the DFARS clause, provide for DoD verification of a contractor's implementation of basic safeguarding requirements or the security requirements specified in NIST SP 800-171 prior to contract award.

Assessing Contractor Implementation of Cybersecurity Requirements

DFARS Case 2019-D041: Interim Rule

November 30, 2020

DFARS 252.204-7019 (Provision)

Notice of NIST SP 800-171 DoD Assessment Requirements

DFARS 252.204-7020 (Clause)

NIST SP 800-171 DoD Assessment Requirements

DFARS 252.204-7021 (Clause)

Cybersecurity Maturity Model Certification Requirements

Top five NAICS code industries expected to be impacted:

- **541712**: Research and Development in the Physical, Engineering, and Life Sciences
- **541330**: Engineering Services
- **236220**: Commercial and Institutional Building Construction
- **541519**: Other Computer Related Services
- **561210**: Facilities Support Services.

These NAICS codes were selected based on a review of NAICS codes associated with awards that include the clause at DFARS 252.204-7012.

DEFCERT

Assessing Contractor Implementation of Cybersecurity Requirements

DFARS Case 2019-D041: Interim Rule

November 30, 2020

DFARS 252.204-7019 (Provision)

Notice of NIST SP 800-171 DoD Assessment Requirements

- Advises of requirements
- Added to all solicitations and contracts

DFARS 252.204-7020 (Clause)

NIST SP 800-171 DoD Assessment Requirements

- If required to implement 800-171 pursuant to DFARS 252.204-7012, then must have current assessment score on record in SPRS
- Basic, Medium, & High Assessments
- Added to all solicitations and contracts
- Requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment.

DEFCERT

November 30, 2020

DFARS 252.204-7019 (Provision)

Notice of NIST SP 800-171 DoD Assessment Requirements

DFARS 252.204-7020 (Clause)

NIST SP 800-171 DoD Assessment Requirements

- A contractor should already be aware of the security requirements they have not yet implemented and have documented plans of action for those requirements.
- Therefore, the burden associated with conducting a self-assessment is the time burden associated with calculating the score:

30 Minutes

DEFCERT

November 30, 2020

DFARS 252.204-7019 (Provision)

Notice of NIST SP 800-171 DoD Assessment Requirements

DFARS 252.204-7020 (Clause)

NIST SP 800-171 DoD Assessment Requirements

While these are rather simple tasks that can reasonably be completed by a GS-11 equivalent employee, or even a GS-9 clerk, the GS-13 (or perhaps GS-11) is the most likely grade for several reasons.

1. First, in a small company, the number of IT personnel are very limited. The employee that is available to complete this task would also have significant responsibilities for operation and maintenance of the IT system and, therefore, be at a higher grade than would otherwise be required if the only job was to prepare and submit the assessment.

2. Second, while the calculation of the assessment is simple, the personnel who would typically have access to and understand the system security plan and plans of action in order to complete the Basic Assessment would be at the higher grade.

3. Third, while the actual submission is a simple task, the person who would complete the assessment and submit the data in SPRS would be the person with SPRS access/responsibilities, and therefore at the higher grade.

4. **Fourth, given that proper calculation of the score and its submission may well determine whether or not the company is awarded the contract, the persons preparing and submitting the report are likely to be at a higher grade than is actually required to ensure this is done properly.**

November 30, 2020

DFARS 252.204-7021 (Clause)

Cybersecurity Maturity Model Certification Requirements

- Will apply to all DoD solicitations and contracts after October 1, 2025.
- Required for contract award/option.
- Requires a contractor to ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments.
- In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level.

November 30, 2020

DFARS 252.204-7021 (Clause)

Cybersecurity Maturity Model Certification Requirements

The estimated costs attributed to this rule do not include the costs associated with compliance with the existing cybersecurity requirements under the clause at FAR 52.204-21 or associated with implementing NIST SP 800-171 in accordance with the clause at DFARS 252.204-7012.

Contractors who have been awarded a DoD contract that include these existing contract clauses should have already implemented these cybersecurity requirements and incurred the associated costs; therefore, those costs are not attributed to this rule.

The rollout is intended to minimize the financial impacts to the industrial base, especially small entities, and disruption to the existing DoD supply chain.

November 30, 2020

DFARS 252.204-7021 (Clause)

Cybersecurity Maturity Model Certification Requirements

Level 1 Certification

- Level 1 Assessment or recertification is **$2,999.56** (small entity):
  - Contractor Support: one employee 14 hours **$1,166.48.**
  - C3PAO Assessment: one assessor 19 hours **$1,833.08.**

Contractors pursuing a Level 1 Certification should have already implemented the 15 existing basic safeguarding requirements under FAR clause 52.204-21.Therefore, there are no estimated nonrecurring or recurring engineering costs associated with CMMC Level 1.

DEFCERT

November 30, 2020

DFARS 252.204-7021 (Clause)

Cybersecurity Maturity Model Certification Requirements

Level 2 Certification

- Level 2 Assessment or recertification: **$22,466.88** (small entity):
  - Contractor Support: Two employees 48 hours each **$11,239.68.**
  - C3PAO Assessment: Two assessors 45 hours each **$11,227.20.**
- Nonrecurring engineering cost: **$8,135**.
- Recurring engineering cost: **$20,154** per year.

Contractors pursuing a Level 2 Certification should have already implemented the 65 existing NIST SP 800-171 security requirements.

Therefore, the estimated engineering costs per small entity is associated with implementation of 9 new requirements (7 CMMC practices and 2 CMMC processes).

The phased rollout estimates that approximately 10% of small entities may choose to use Level 2 as a transition step from Level 1 to Level 3.

The Department does not anticipate releasing new contracts that require contractors to achieve CMMC Level 2.

DEFCERT

November 30, 2020

DFARS 252.204-7021 (Clause)

Cybersecurity Maturity Model Certification Requirements

Level 3 Certification

- Level 3 assessment or recertification: **$51,095.60** (small entity):
  - Contractor Support: three employees 64 hours each **$22,479.36.**
  - C3PAO Assessment: Four assessors 57 hours each **$28,616.24.**
- Nonrecurring engineering cost: **$26,214**.
- Recurring engineering cost: **$41,666** per year.

Contractors pursuing a Level 3 Certification should have already implemented the 110 existing NIST SP 800-171 security requirements.

Therefore, the estimated engineering costs per small entity is associated with implementation 23 new requirements (20 CMMC practices and 3 CMMC processes).

DEFCERT

A Timeline of Assumptions

May 2015
Federal CUI Program
Proposed Rule – 32 CFR 2002

Sep 2016
Federal CUI Program
Final Rule – 32 CFR 2002

Mar 2010
DFARS "RFC"
DFARS Case
2008-D028

Jun 2011
Proposed Rule
DFARS Case
2011-D039

Nov 2013
Final Rule
DFARS Case
2011-D039

Aug 2015
Interim Rule
DFARS Case
2011-D018

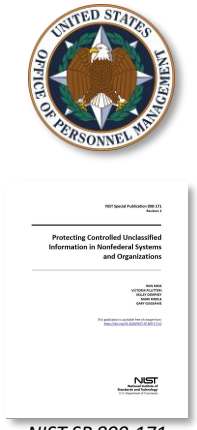
Dec 2015
Interim Rule
DFARS Case
2011-D018

Oct 2016
Final Rule
DFARS Case
2011-D018

Nov 2020
Interim Rule
DFARS Case
2019-D041

Nov 2010

Jun 2015



NIST SP 800-171

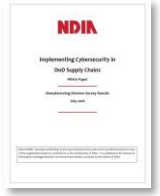
Jul 2017

E.O. 13806

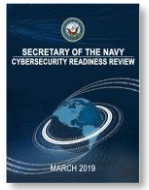
Jun 2018

SEADRAGON

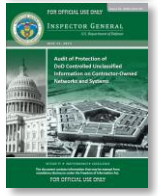
Summer 2018



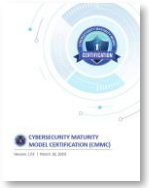
Spring 2019



Summer 2019



Mar 2020



Dec 2020

SUNBURST

Feb 2021

E.O. 14017

Aug 2012
Proposed Rule
FAR Case 2011-020

Jun 2016
Final Rule
FAR Case 2011-020

July 2015
FAR CUI Rule
OMB "RFC"

DEFCERT

A Timeline of Assumptions

May 2015

Federal CUI Program
Proposed Rule – 32 CFR 2002

Sep 2016

Federal CUI Program
Final Rule – 32 CFR 2002

Mar 2010

DFARS "RFC"
DFARS Case
2008-D028

Jun 2011

Proposed Rule
DFARS Case
2011-D039

Nov 2013

Final Rule
DFARS Case
2011-D039

Aug 2015

Interim Rule
DFARS Case
2011-D018

Dec 2015

Interim Rule
DFARS Case
2011-D018

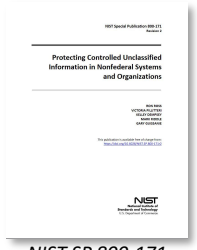
Oct 2016

Nov 2020

Nov 2010


Executive Order 13556 -- Controlled Unclassified Information

Jun 2015


Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST SP 800-171

Dec 2020

SUNBURST

Feb 2021


Executive Order on America's Supply Chains

E.O. 14017

Aug 2012

Proposed Rule
FAR Case 2011-020

Jun 2016

Final Rule
FAR Case 2011-020

July 2015

FAR CUI Rule
OMB "RFC"

DEFCERT

Common Assumptions

Assumptions to Avoid

- Only 130 Technical Requirements.
- Scope of DFARS Cybersecurity = NIST SP 800-171.
- SPRS “Implemented” = CMMC Assessable.

- CMMC is going away.
- The CMMC Accrediting Body is in charge.
- There will be monetary relief.

- Your managed IT service provider (“MSP”) has things under control.
- Your customers will provide scalable, compliant infrastructure.
- You don’t have to flow down.

DEFCERT

Key Takeaways

- Cost is a function of the scope of your *covered contractor information system*.
- The scope of your covered contractor information system is a function of how CUI and FCI flows through your business.
- Evaluate vendors, technologies, and consultants on whether they provide scope assessments rather than just “gap assessments”.

DEFCERT

“Security is an allowable cost. We need you to build it into your rate. If you go to the Federal Register, we put in very clearly what we thought were good estimates on how much it would cost. We took into consideration how long we thought it would take a company to prepare and the cost to do that (to prepare for the audit). To actually have the audit and then the clean up from the audit to make sure that they got everything done. So, we included that, so we want you to build that into your rate.”

- Katie Arrington, February 17th, 2021

DEFCERT

DEFCERT

COMPLIANCE IN CONTEXT

jacob.horne@defcert.com
www.defcert.com