A Banquet of Consequences

The Story of CUI, DFARS, and CMMC

DEFCERT

A Banquet of Consequences

The Story of CUI, DFARS, and CMMC

DEFCERT

Chapter 1

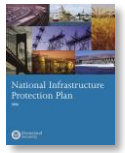
The Post 9/11 Commission Report through Executive Order 13556

"The executive establishment developed without a plan or design like barns, shacks, silos, tool sheds, and garages of an old farm."

- The Brownlow Committee, 1937

DEFCERT

Parallel Timelines



Dec 2003 — HSPD-7

Jan 2006 — NIPP

May 2007 — DIB CA/IA

Mar 2010 — DFARS Case 2008-D028

Nov 2002 — Homeland Security Act

Dec 2004 — Intel. Reform & Terrorism Prevention Act

Dec 2005 — Presidential Memorandum

May 2008 — Presidential Memorandum

May 2009 — Presidential Memorandum

Aug 2009 — Presidential Task Force on CUI

Nov 2010 — Executive Order 13556

Dec 2002 — Federal Information Security Management Act

Feb 2004 — FIPS 199

Feb 2005 — NIST SP 800-53

Mar 2006 — FIPS 200

DEFCERT

Three Elements of the Executive Order

1 Federal CUI Rule

- 15 Departments
- 78 Agencies
- 173 Bureaus

Nov 2010

Executive Order 13556

2 Security Requirements for Non-Federal Systems

Contracting Base

3 FAR CUI Rule

FAR
AGAR
GSAM/R
Ch. 99 (CAS)
AIDAR
HHSAR
DFARS
CAR
HSAR
DFARSPGI
DEAR
HUDAR
AFARS
DIAR
IAAR
AFFARS
DOLAR
JAR
DARS
DOSAR
LIFAR
DLAD
DTAR
NFS
NMCARS
EDAR
NRCAR
SOFARS
EPAAR
TAR
TRANSFARS
FEHBAR
VAAR

DEFCERT

Organizational Debt Delays the Sequence of EO Implementation

1 Federal CUI Rule

2 Security Requirements for Non-Federal Systems

3 FAR CUI Rule

ORGANIZATIONAL DEBT

Nov 2010

Executive Order 13556

Sep 2016

Final Rule 32 CFR 2002

Who Protects What, Why, & How

- Who: 170+ Departments, Agencies, Bureaus
- What & Why: CUI Registry
- How: 32 CFR 2002

The Ultimate De-Duplication Effort

- 2,200+ Laws, regulations, government-wide policies
- 150+ Safeguarding and dissemination control markings
- Now: singular marking guidance and authoritative registry

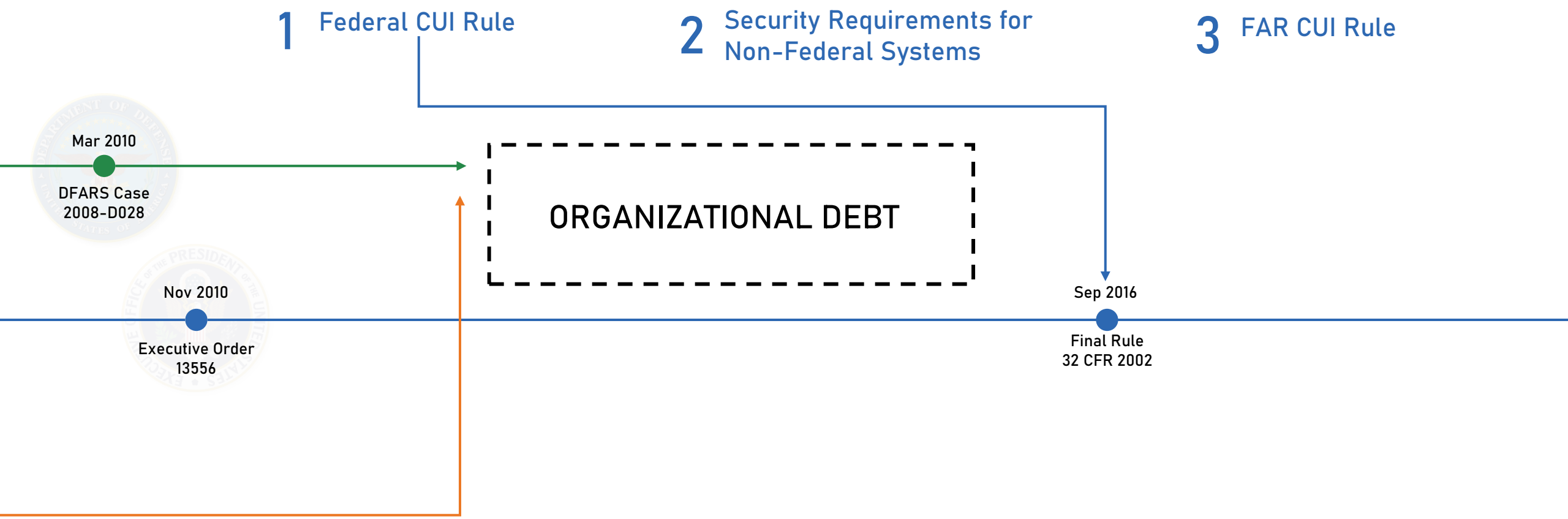
NATIONAL ARCHIVES

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION 1985 LITTERA SCRIPTA MANET

DEFCERT

Source: ISOO Open House 2016
https://www.youtube.com/watch?v=UJkNGlTQbA0&t=2593s

Timelines Converge in the Gap Left by Organizational Debt



DEFCERT

Chapter 2

DoD Rulemaking 2010 – 2013

"The right understanding of any matter and a misunderstanding of the same matter do not wholly exclude each other."

- Franz Kafka, *The Trial*

March 2010 – DoD Advanced Notice of Public Rulemaking

DFARS 252.204-7XXX

Basic Safeguarding of Unclassified Information Within Industry

Relevant Data Types

Any unclassified DoD information not cleared for public release

Basic Safeguarding Requirements

- Designation
- Public Resources/Sites
- Transmitting electronic information
- Transmitting voice/fax information
- Physical and electronic barriers
- Intrusion Protection
- Malware Protection
- Patch Management
- Send only to need-to-know
- Sanitization

DFARS 252.204-7YYY

Enhanced Safeguarding of Unclassified Information Within Industry

Relevant Data Types

- Critical Program Information (CPI)
- ITAR/EAR
- FOIA Exempt
- Controlled Access/Dissemination Markings
- Distribution Statements (DoDI 5230.24)
- PII/PHI

Enhanced Safeguarding Requirements

- Encryption
- Network Intrusion Protection
- Anti-malware
- Monitor & control traffic
- Patch management
- Tailor and implement 800-53
- Cyber Intrusion Reporting
- Incident reporting w/ in 72 hours
- Support forensic analysis
- Support damage assessment
- Preserve and protect images indefinitely
- Cooperate and provide further access

"These changes to the DFARS address requirements for the safeguarding of unclassified information and may be altered as necessary to align with any future direction given in response to on-going efforts currently being led by the National Archives and Records Administration regarding Controlled Unclassified Information (CUI)."

DEFCERT

Source: DFARS Case 2008-D028

June 2011 – Proposed Rule

DFARS 252.204-70XX

Basic Safeguarding of Unclassified Information Within Industry

Relevant Data Types

Any unclassified DoD information not cleared for public release

Cost Impact: "Not Significant"

- "First-level" protective measures are typically employed as part of the routine course of doing business.
- Security protections are prudent business practice.
  - Typically, a common part of everyday operations.
- The cost of not using basic security measures would be an enormous detriment to contractor and DoD business:
  - Reduced system performance
  - Potential loss of valuable information
- As a result, securely receiving and processing DoD information offers enormous value to contractors and DoD:
  - Reducing vulnerabilities in contractor systems.
  - Preventing data exfiltration.

DFARS 252.204-70YY

Enhanced Safeguarding of Unclassified Information Within Industry

Relevant Data Types

- Critical Program Information (CPI)
- ITAR/EAR
- FOIA Exempt
- Controlled Access/Dissemination Markings
- Distribution Statements (DoDI 5230.24)
- PII/PHI
- OPSEC

Cost Impact: Relative

- Most large contractors already have sophisticated security programs and can take credit for existing controls with minimal cost.
- Most small businesses have less sophisticated programs and will realize cost meeting the additional requirements.
- Economies of scale: "larger businesses generally pay only a fraction of estimated cost as a percentage of total revenue."
- Reasonable rule of thumb: small business IT security costs are approximately: 0.5% of total revenues.

DEFCERT

Source: DFARS Case 2011-D039

June 2011 – Proposed Rule

59 Controls from NIST SP 800-53

Access Control	Awareness & Training	Audit & Accountability	Configuration Management	Contingency Planning	Identification & Authentication	Incident Response	Maintenance	Media Protection	Physical & Env. Safeguards	Program Management	System & Comms. Protection	System & Information Integrity
AC-2	AT-2	AU-2	CM-2	CP-9	IA-2	IR-2	MA-4	MP-4	PE-5	PM-10	SC-2	SI-2
AC-3		AU-3	CM-6		IA-4	IR-4	MA-4(6)	MP-6	PE-7		SC-4	SI-3
AC-3(4)		AU-6	CM-7		IA-5	IR-5	MA-5				SC-7	SI-4
AC-4		AU-6(1)	CM-8		IA-5(1)	IR-6	MA-6				SC-7(2)	
AC-6		AU-7									SC-9	
AC-7		AU-8									SC-9(1)	
AC-11		AU-9									SC-13	
AC-11(1)		AU-10									SC-13(1)	
AC-17		AU-10(5)									SC-13(4)	
AC-18											SC-15	
AC-18(1)											SC-28	
AC-19												
13	**1**	**9**	**4**	**1**	**4**	**4**	**4**	**2**	**2**	**1**	**11**	**3**

DEFCERT

Source: DFARS Case 2011-D039

November 2013 – Final Rule

DFARS 252.204-7012

Safeguarding of Unclassified Controlled Technical Information

Relevant Data Types

Controlled Technical Information ("CTI") is technical data, computer software, and any other technical information covered by DoD Directive 5230.24 & 5230.25

Rationale

- After comments received on the proposed rule it was decided that the scope of the rule would be modified to reduce the categories of information covered.
- Federal CUI policy has not yet been promulgated for Federal Government agencies. Unknown when Federal policy for CUI will be developed for industry.
- Rule rescoped to cover safeguarding unclassified CTI, which DoD has determined to be of utmost importance and has existing authority to protect.

Cost Impact: Relative

- Most large contractors already have sophisticated security programs and can take credit for existing controls with minimal cost.
- Most small businesses have less sophisticated programs and will realize cost meeting the additional requirements.
- Economies of scale: "larger businesses generally pay only a fraction of estimated cost as a percentage of total revenue."
- Reasonable rule of thumb: small business IT security costs are approximately: 0.5% of total revenues.

Cost Impact Rationale

- Implementing these controls may increase costs to DoD.
- Implementation may increase contractor costs that would be accounted for through the normal course of business.
- Costs are allowable and chargeable to indirect cost pools.
- The Government does not intend to directly pay for the operating costs associated with the rule.
- Data retention period for DC3 investigation/battle damage assessment reduced to 90 days.

DEFCERT

Source: DFARS Case 2011-D039

November 2013 – Final Rule Comment Analysis

These controls aren't risk-based! This burden is closer to classified systems than unclassified!

- The rule does not require adoption of a NIST compliant security program.
- NIST SP 800-53 controls are a reference to the specific security capabilities that a contractor's system should provide.

Small biz has no infrastructure! Compliance is way more expensive on a relative basis!

- The contractor's size classification is not a sufficient reason to allow a contractor to fail to protect technical information.

The costs of compliance are too large!

- NIST 800-53 closely parallels ISO 27002.
- Therefore, the controls represent mainstream industry practices.
- There is cost associated with implementing information assurance controls.
- The use of industry practices provides assurance the costs are reasonable.

Isn't this prone to erroneous inclusion?

- The best means of addressing the identified potential for usage errors is to include the clause in all contracts.
- DFARS 252.204-7012 is now prescribed to go in all contracts and solicitations.
- The additional safeguarding measures will only apply when unclassified CTI is present.
- The purpose of this rule is to protect the noted category of unclassified information
- included whenever such information would potentially be present.

Costs of controls outweigh the benefits!

- Benefits of particular controls are difficult to quantify.
- Not possible to determine the exact point at which benefits equal costs.
- Does not preclude protecting information and accruing the associated costs.

It's challenging to ensure that recipients of CTI also have systems with enhanced safeguarding and adequate security!

- Contractors are obligated to ensure recipients of information requiring enhanced safeguarding are authorized to receive the information, and that it be transferred with the appropriate security.
- It is the responsibility of the authorized recipient to safeguard that information appropriately subject to contractual requirements.
- The contractor is responsible for ensuring that the subcontract complies with the requirements within the scope of this rule.
- Cloud service providers constitute a subcontractor in this context.

This is financially burdensome for small biz! They won't be able to participate! Grossly underestimate cost as a percentage of revenue! A phased-in approach would ease the financial burden!

- No changes were made as a result.
- The estimated burden is reduced because the scope of the rule reduced the categories of information to CTI.
- The final rule is written with the aim of minimizing the burden of compliance on contractors while implementing the necessary safeguarding requirements.

Source: DFARS Case 2011-D039

November 2013 – Final Rule

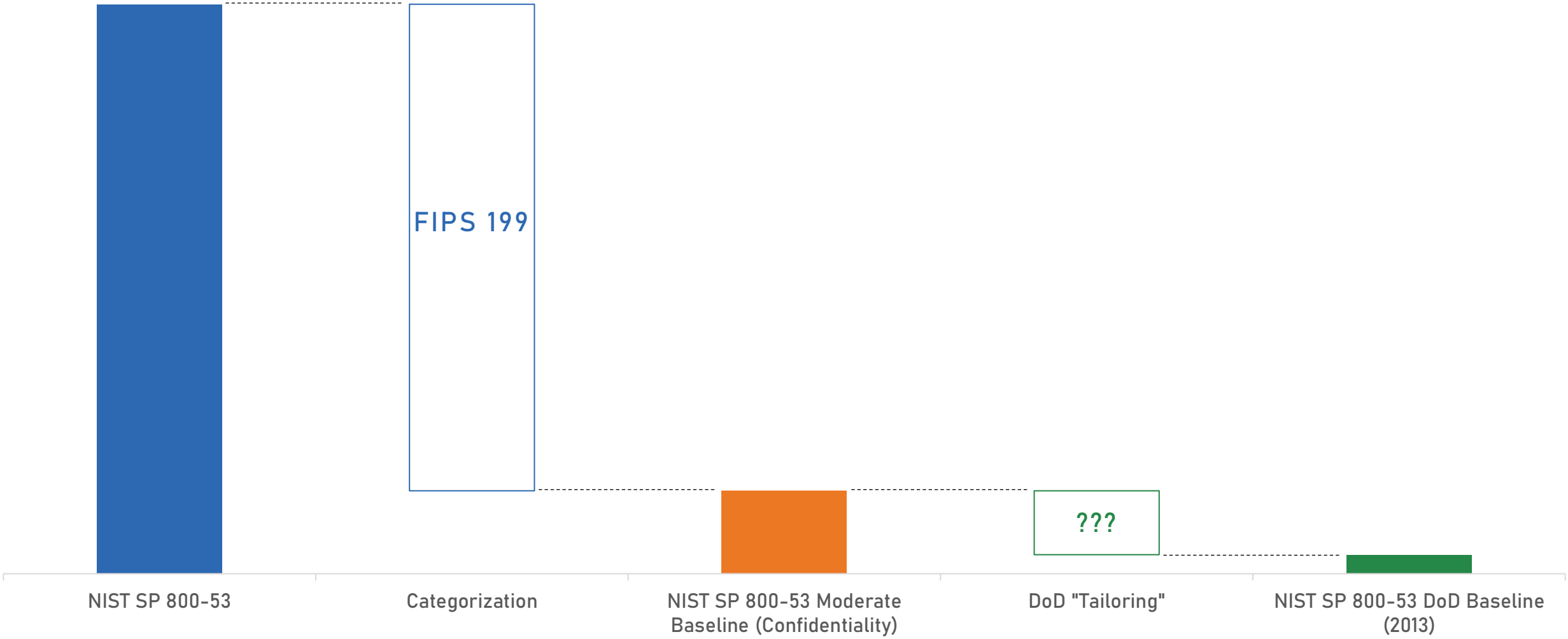
60 Controls from NIST SP 800-53

Access Control	Awareness & Training	Audit & Accountability	Configuration Management	Contingency Planning	Identification & Authentication	Incident Response	Maintenance	Media Protection	Physical & Env. Safeguards	Program Management	Risk Assessment	System & Comms. Protection	System & Information Integrity
AC-2	AT-2	AU-2	CM-2	CP-9	IA-2	IR-2	MA-4	MP-4	PE-2	PM-10	RA-5	SC-2	SI-2
AC-3		AU-3	CM-6		IA-4	IR-4	MA-4(6)	MP-6	PE-3			SC-4	SI-3
AC-3(4)		AU-6	CM-7		IA-5	IR-5	MA-5		PE-5			SC-7	SI-4
AC-4		AU-6(1)	CM-8		IA-5(1)	IR-6	MA-6					SC-8	
AC-6		AU-7										SC-8(1)	
AC-7		AU-8										SC-13	
AC-11		AU-9										SC-15	
AC-11(1)												SC-28	
AC-17													
AC-17(2)													
AC-18													
AC-18(1)													
AC-19													
AC-20													
AC-20(1)													
AC-20(2)													
AC-22													
17	**1**	**7**	**4**	**1**	**4**	**4**	**4**	**2**	**3**	**1**	**1**	**8**	**3**

DEFCERT

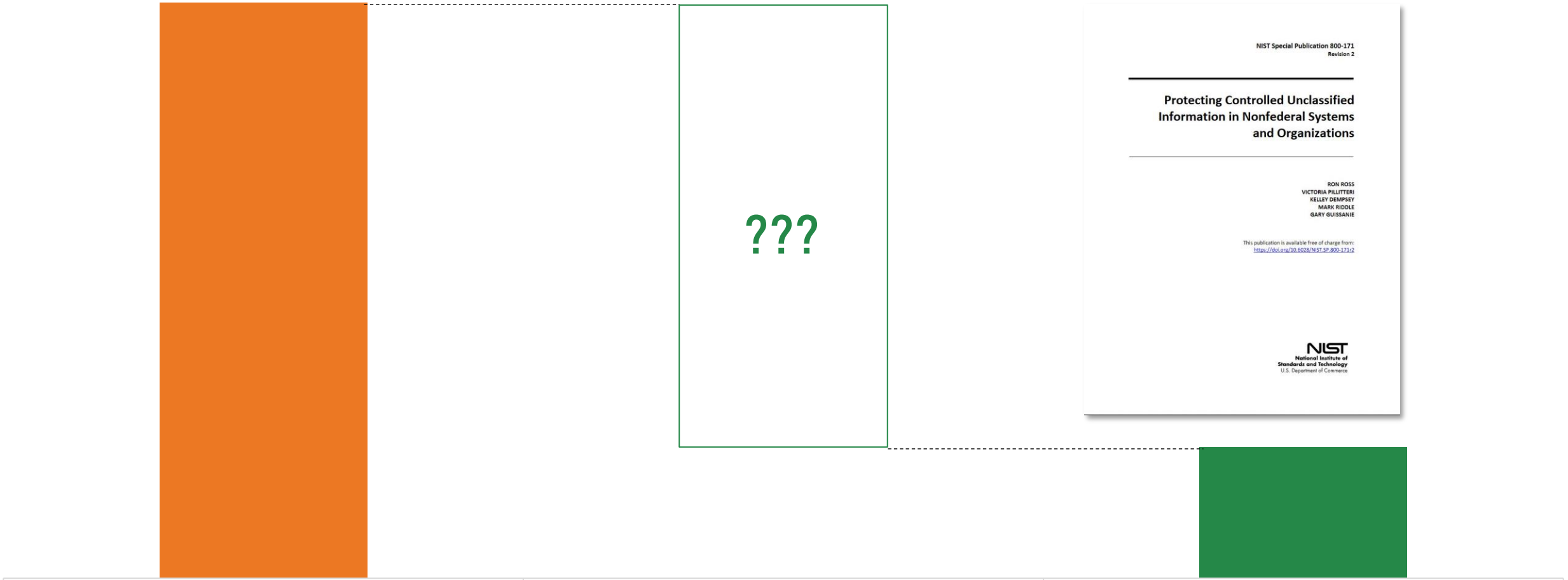
Source: DFARS Case 2011-D039

NIST & NARA Protest DoD Control Baseline (2013)



DEFCERT

NIST & NARA Protest DoD Control Baseline (2013)



NIST SP 800-53 Moderate Baseline (Confidentiality)

DoD "Tailoring"

NIST SP 800-53 DoD Baseline (2013)

DEFCERT

Chapter 3

DoD Rulemaking 2015 – 2018

“Sooner or later, everyone sits down to a banquet of consequences.”

- Robert Louis Stevenson

DEFCERT

Development of NIST SP 800-171

> We were looking at putting ourselves in the place of a nonfederal organization. So, it isn't like the private sector is doing nothing with regard to cybersecurity – they are doing a lot because they have critical missions and business operations just like we do and they're using the same technology. They're subject to cyber attacks just like we are. They're information is subject to a high level of risk just like ours is. So, we made some assumptions…

Dr. Ron Ross, June 26th, 2015
NIST Fellow

NIST SP 800-53 Moderate Baseline (Confidentiality)

FED
Uniquely Federal, primarily the responsibility of the Federal Government.

NCO
Not directly related to protecting the confidentiality of CUI.

NFO
Expected to be routinely satisfied by non-federal organizations without specification.

FIPS 200

NIST SP 800-171 Requirements

Source: ISOO Open House Session 2 of 4
https://www.youtube.com/watch?v=dAB8OfbpmiY&t=2s

Development of NIST SP 800-171

> 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.

Dr. Ron Ross, June 26th, 2015
NIST Fellow

NIST SP 800-53 Moderate Baseline (Confidentiality)

FED
Uniquely Federal, primarily the responsibility of the Federal Government.

NCO
Not directly related to protecting the confidentiality of CUI.

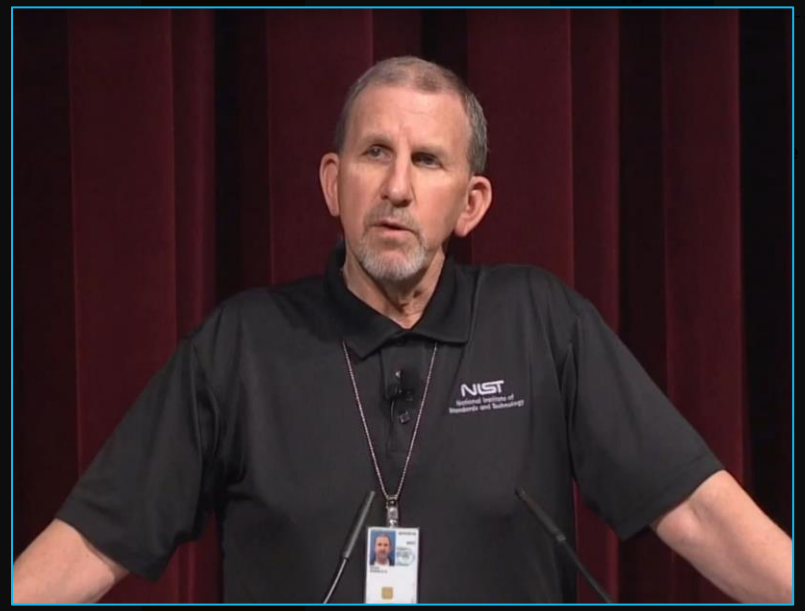
NFO
Expected to be routinely satisfied by non-federal organizations without specification.

FIPS 200

NIST SP 800-171 Requirements

Source: ISOO Open House Session 2 of 4
https://www.youtube.com/watch?v=dAB8OfbpmiY&t=2s

Development of NIST SP 800-171



> We assume they have some level of protection in place. Whether they are using the NIST catalog of controls or using ISO 27001 or the new CSF – they're protecting their stuff because they have to in order to stay in business.

Dr. Ron Ross, June 26th, 2015
NIST Fellow

NIST SP 800-53 Moderate Baseline (Confidentiality)

FED
Uniquely Federal, primarily the responsibility of the Federal Government.

NCO
Not directly related to protecting the confidentiality of CUI.

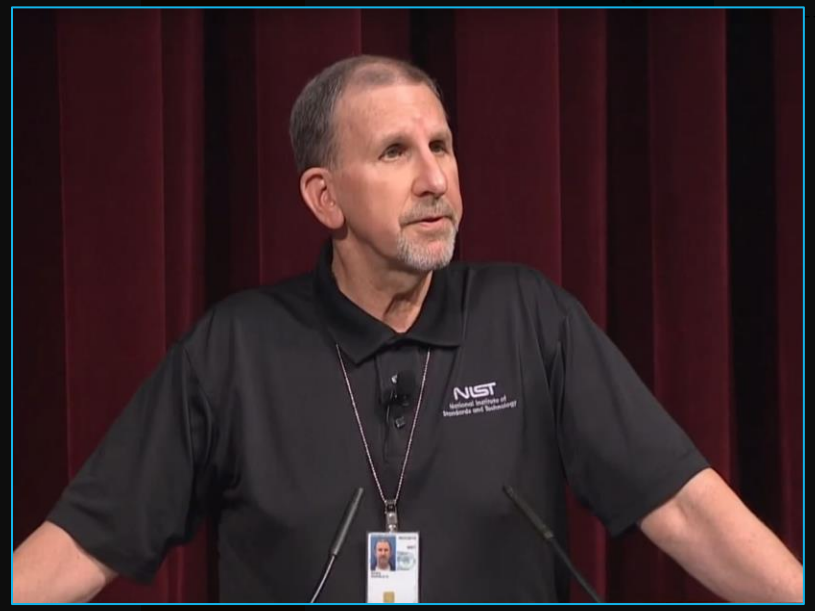
NFO
Expected to be routinely satisfied by non-federal organizations without specification.

FIPS 200

NIST SP 800-171 Requirements

Source: ISOO Open House Session 2 of 4
https://www.youtube.com/watch?v=dAB8OfbpmiY&t=2s

Development of NIST SP 800-171



> 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, June 26th, 2015
NIST Fellow

NIST SP 800-53 Moderate Baseline (Confidentiality)

FED
Uniquely Federal, primarily the responsibility of the Federal Government.

NCO
Not directly related to protecting the confidentiality of CUI.

NFO
Expected to be routinely satisfied by non-federal organizations without specification.

FIPS 200

NIST SP 800-171 Requirements

Source: ISOO Open House Session 2 of 4
https://www.youtube.com/watch?v=dAB8OfbpmiY&t=2s

Development of NIST SP 800-171

> We went through and took a hard look and said, 'Do you think we have to tell people to do this? Or should that kind of be 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, June 26th, 2015
NIST Fellow

NIST SP 800-53 Moderate Baseline (Confidentiality)

FED
Uniquely Federal, primarily the responsibility of the Federal Government.

NCO
Not directly related to protecting the confidentiality of CUI.

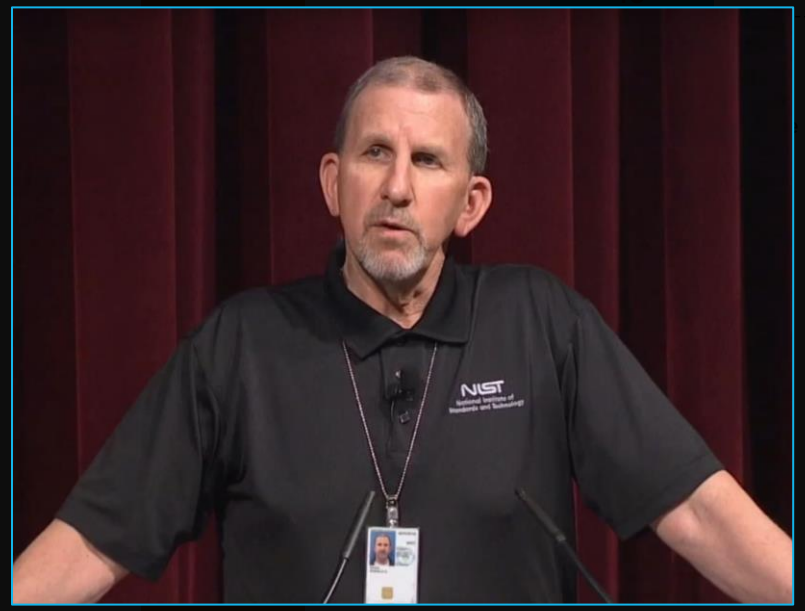
NFO
Expected to be routinely satisfied by non-federal organizations without specification.

FIPS 200

NIST SP 800-171 Requirements

Source: ISOO Open House Session 2 of 4
https://www.youtube.com/watch?v=dAB8OfbpmiY&t=2s

Development of NIST SP 800-171

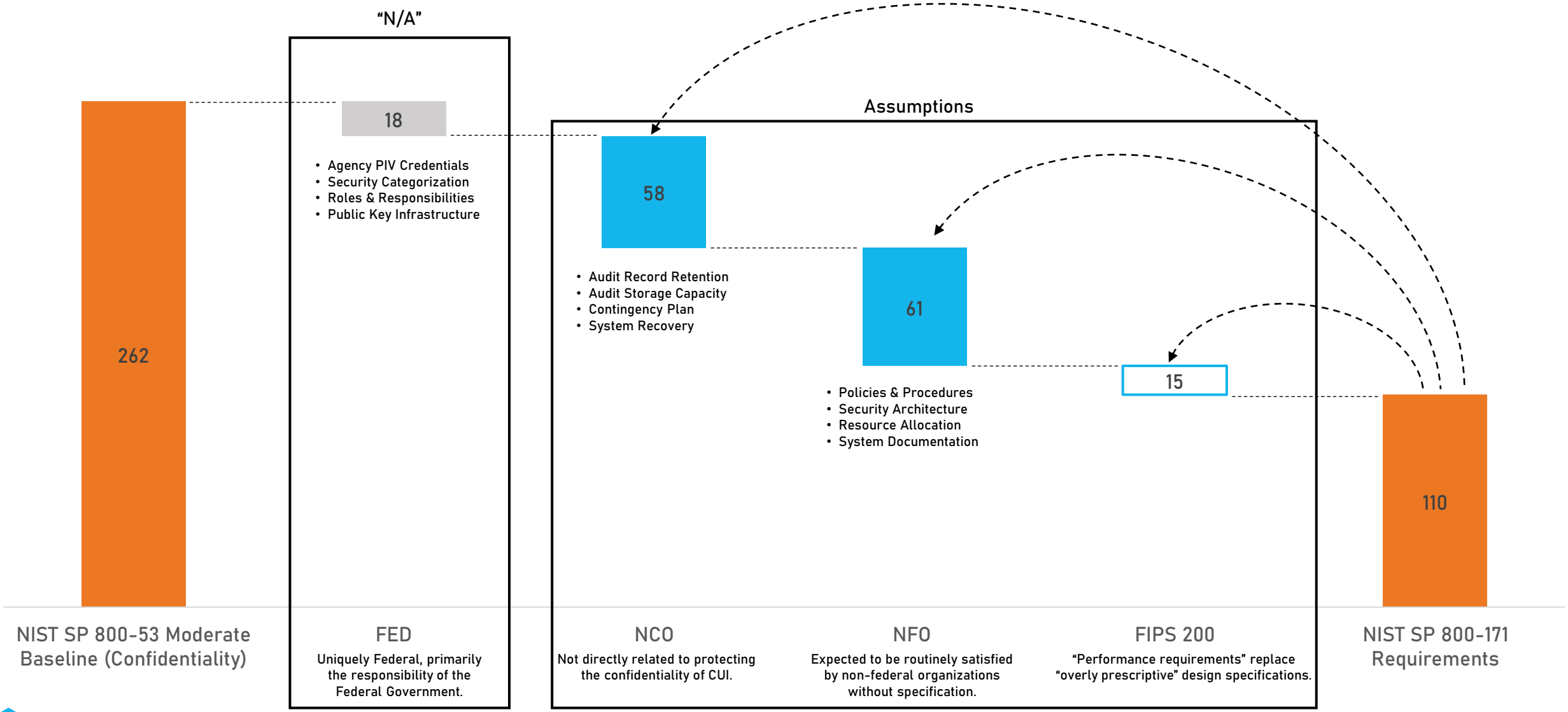


> Now, it could happen that some of our assumptions, the things that we thought they were doing – they may not be doing. But again, we had to make some design decisions on how these requirements came out.

Dr. Ron Ross, June 26th, 2015
NIST Fellow

Source: ISOO Open House Session 2 of 4
https://www.youtube.com/watch?v=dAB8OfbpmiY&t=2s

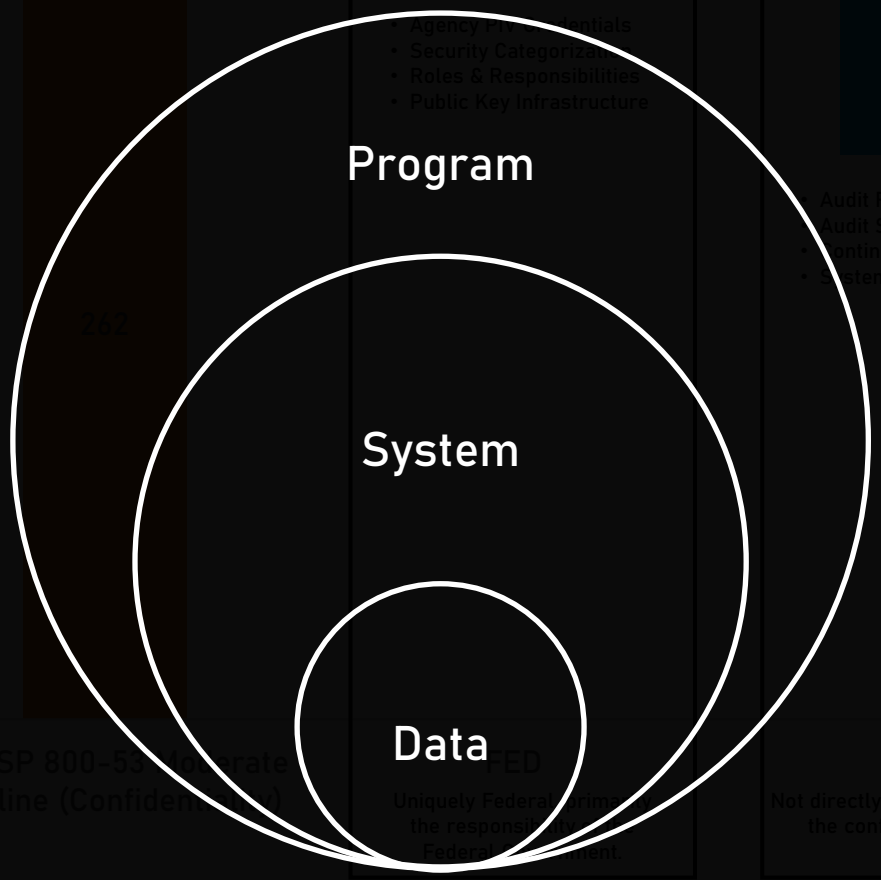
Tailoring NIST SP 800-171



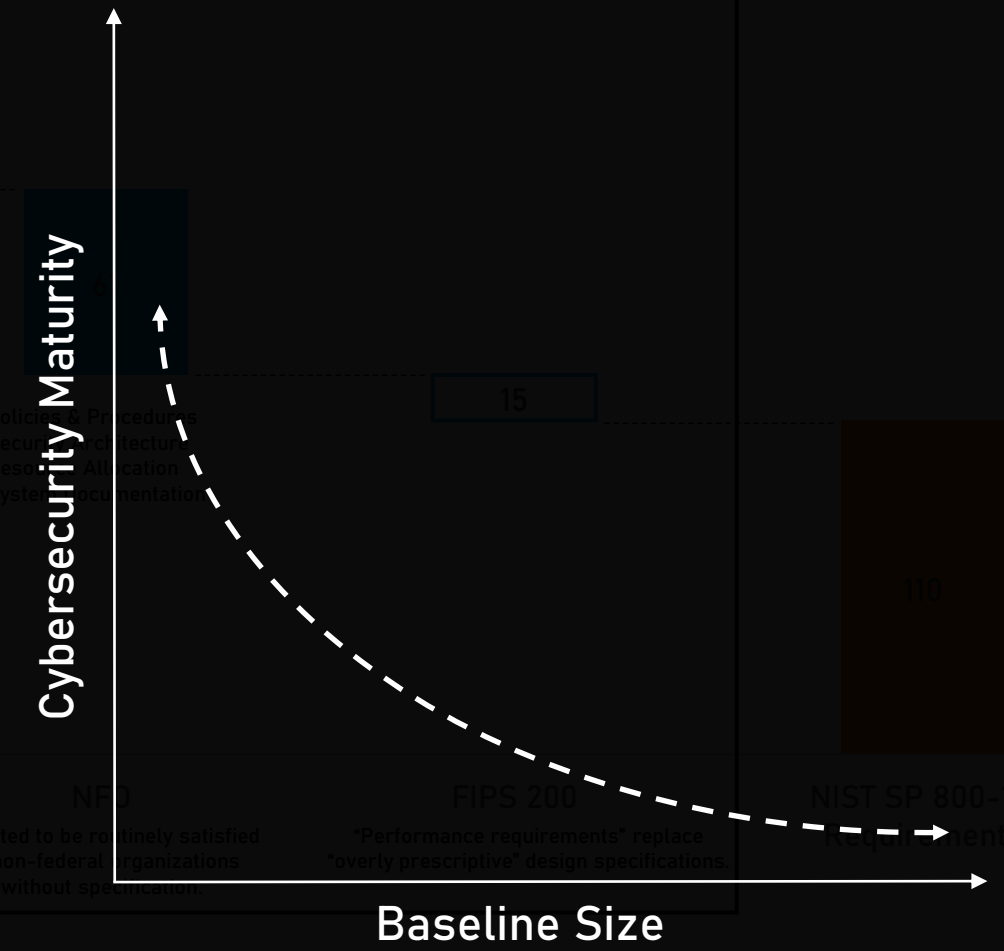
Source: NIST SP 800-171 rev. 2 Appendix E

Tailoring NIST SP 800-171

Tailoring Removes Program Inputs



Tailoring Assumes Maturity



Source: NIST SP 800-171 rev. 2 Appendix E

> Initially the System Security Plan was listed as [NFO] because you had to have something like that to build your system. So, we didn't want to be bureaucratic and say, 'you have to have a system security plan'.
>
> Then, as the DFARS began to be implemented we got an endless number of questions about [documentation] and we found it very difficult to continue to say that when it wasn't really explicit in 171."

Gary Guissanie, October 18th, 2018
Adjunct Research Staff Member
Institute for Defense Analysis

Special Publication 800-171 — Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Table E-12: Tailoring Actions for Planning Controls

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PL-1	Security Planning Policy and Procedures	NFO
PL-2	System Security Plan	NFO
PL-2(3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	NFO
PL-4	Rules of Behavior	NFO
PL-4(1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*	NFO
PL-8	Information Security Architecture	NFO

June 2015

Special Publication 800-171 Revision 1 — Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Table E-12: Tailoring Actions for Planning Controls

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
PL-1	Security Planning Policy and Procedures	NFO
PL-2	System Security Plan	CUI
PL-2(3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	NFO
PL-4	Rules of Behavior	NFO
PL-4(1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*	NFO
PL-8	Information Security Architecture	NFO

December 2016

Source: Controlled Unclassified Information Security Requirements Workshop
https://www.nist.gov/news-events/events/2018/10/controlled-unclassified-information-security-requirements-workshop

August 2015 – Interim Rule

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

Key Points

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

Features

- NIST SP 800-171 replaces 800-53, reduces required tasks by: 30%
- "Several of the required [incident] reporting fields will likely require an IT expert to describe or at least to determine what information was affected."

Relevant Data Types

Scope expanded to safeguarding and reporting for:

- Covered Contractor Information Systems
- Covered Defense Information ("CDI")

Covered Defense Information

- Unclassified information that –
  - Is –
    - Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or
    - Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and
  - Falls into any of the following categories:
    - Controlled Technical Information
    - OPSEC
    - Export Control
    - Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.

DEFCERT

Source: DFARS Case 2013-D018

November 2016 – Final Rule

DFARS 252.204-7008 (Provision)

Compliance with Safeguarding Covered Defense Information Controls

DFARS 252.204-7012 (Clause)

Safeguarding Covered Defense Information & Cyber Incident Reporting

Key Points

- Cloud Service Providers that store, process, or transmit CDI must meet FedRAMP moderate equivalency.

Features

- COTS Exemption reduces the impact on small business.
- The need to protect CDI does not change when such information is shared with nonfederal partners including small business.

Relevant Data Types

Scope expanded to safeguarding and reporting for:

- Covered Contractor Information Systems
- Covered Defense Information ("CDI")

NIST SP 800-171

- Reduces the burden placed on contractors by eliminating Federal-centric requirements and unnecessary specificity.
- Builds upon the table of controls contained in the November 2013 version of DFARS clause 252.204-7012.
- Includes only those requirements necessary to provide adequate protections for the impact level of CUI.
- Provides significant benefit to the small business community through increased protection of their IP.

Ask DoD CIO for "N/A" or Variances

- The basis for determining acceptability of an alternative to a security requirement is whether the alternative is equally effective.
- The basis for determining applicability is whether the basis or condition for the requirement is absent.

DEFCERT

Source: DFARS Case 2013-D018

November 2016 – Final Rule Comment Analysis

Too expensive! There should be an alternative approach for small businesses!

- Alternative Paths Considered for Small Entities:
  - An Exemption
  - Delaying for further cost analysis
  - Creating a different set of security requirements
- Rejected. Conflicts with the overarching purpose of this rule: 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 needs to be the same across the board.
- The value of the information (and impact of its loss) does not diminish when it moves to contractors (prime or sub, large or small).

Small business is unable to afford the investment!

- The cost of compliance with the requirements of this rule is unknown.
- Cost is based on the make-up of the information system and the current state of security already in place.
- For new contractors not yet subject to the previous iteration of clause 252.204-7012 the cost could be significant to comply.

No Oversight?

- The rule does not require "certification" of any kind. By signing the contract, the contractor agrees to comply with the contract's terms.

DoD should provide services or subsidies to cover consultation costs!

- 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.
- The cost of compliance is allowable and should be accounted for in proposal pricing.
- There is no funding appropriation attached to compliance with the rule, so it is not feasible to create a program for compliance or a one-time subsidy related to the new security requirements associated with the rule.

Source: DFARS Case 2013-D018

> There's been experience in the Department in other areas where - I think the term is "creating a cottage industry of non-value-added … stuff". We've had experience with 3rd party assessments before and it's not worked out well.

Gary Guissanie, October 18th, 2018
Adjunct Research Staff Member
Institute for Defense Analysis

> It creates an industry where we're not sure we need to create one. Because there exists, in many businesses, the cybersecurity knowledge and ability to protect their proprietary information because they've been doing so for years. We don't want to introduce a middleman certification between industry and the government about compliance where it's not absolutely necessary.

Devin Casey, October 18th, 2018
Fmr. Program Analyst, Controlled Unclassified Information
Information Security Oversight Office, NARA

Source: Controlled Unclassified Information Security Requirements Workshop
https://www.nist.gov/news-events/events/2018/10/controlled-unclassified-information-security-requirements-workshop

Chapter 4

Self-Attestation in the Defense Industrial Base 2018 - 2021

"I'm shocked, shocked to find out there's gambling going on in here."

- Captain Louis Renault, *Casablanca*

A Timeline of Assumptions

DFARS Rulemaking

Mar 2010 — ANPR DFARS Case 2008-D028

Jun 2011 — Proposed Rule DFARS Case 2011-D039

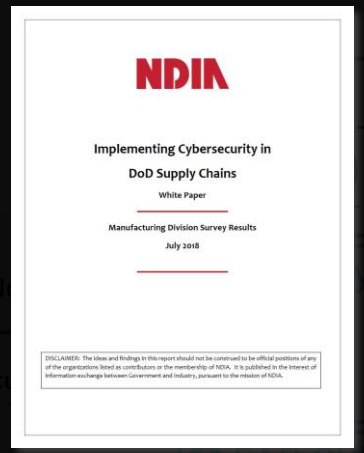
Nov 2013 — Final Rule DFARS Case 2011-D039

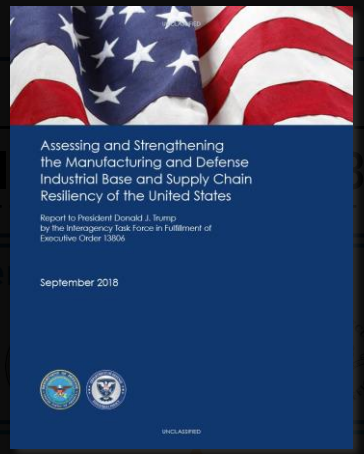
Aug 2015 — Interim Rule DFARS Case 2013-D018

Dec 2015 — Interim Rule DFARS Case 2013-D018

Oct 2016 — Final Rule DFARS Case 2013-D018

Dec 2017 — NIST SP 800-171 Implementation Deadline





FAR "Basic"

Aug 2012 — Proposed Rule FAR Case 2011-020

Jun 2016 — Final Rule FAR Case 2011-020

A Timeline of Assumptions

DFARS Rulemaking

Mar 2010 — ANPR DFARS Case 2008-D028

Jun 2011 — Proposed Rule DFARS Case 2011-D039

Nov 2013 — Final Rule DFARS Case 2011-D039

Aug 2015

Dec 2015

Oct 2016 — Final Rule DFARS Case 2013-D018

Dec 2017 — NIST SP 800-171 Implementation Deadline

1 Federal CUI Rule

ORGANIZATIONAL DE

Sep 2016 — Final Rule 32 CFR 2002

2 Security Requirements

Nov 2010 — Executive Order 13556

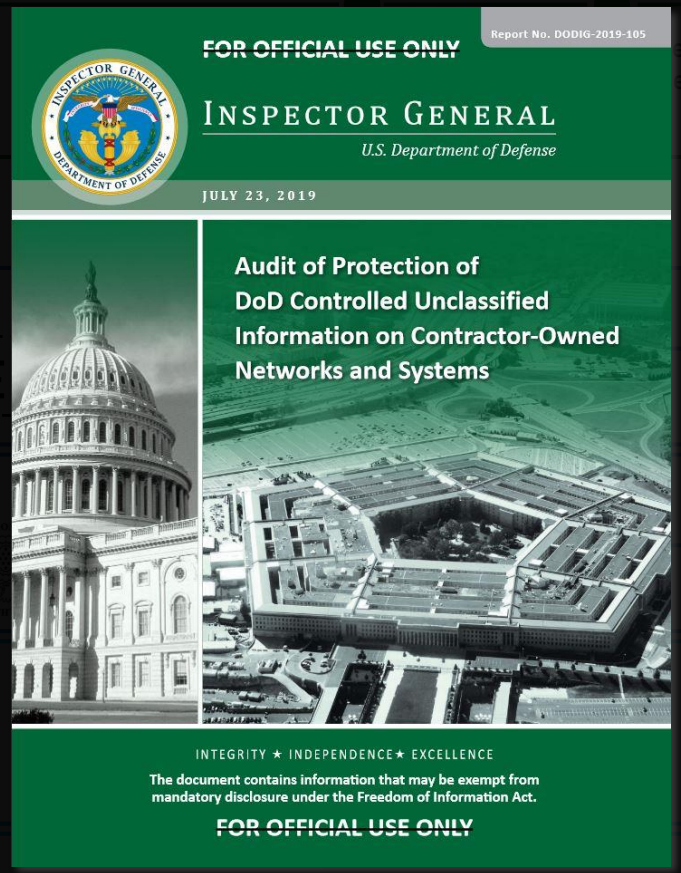
Dec 2016 — NIST SP 800-171 rev 1

3 FAR CUI Rule

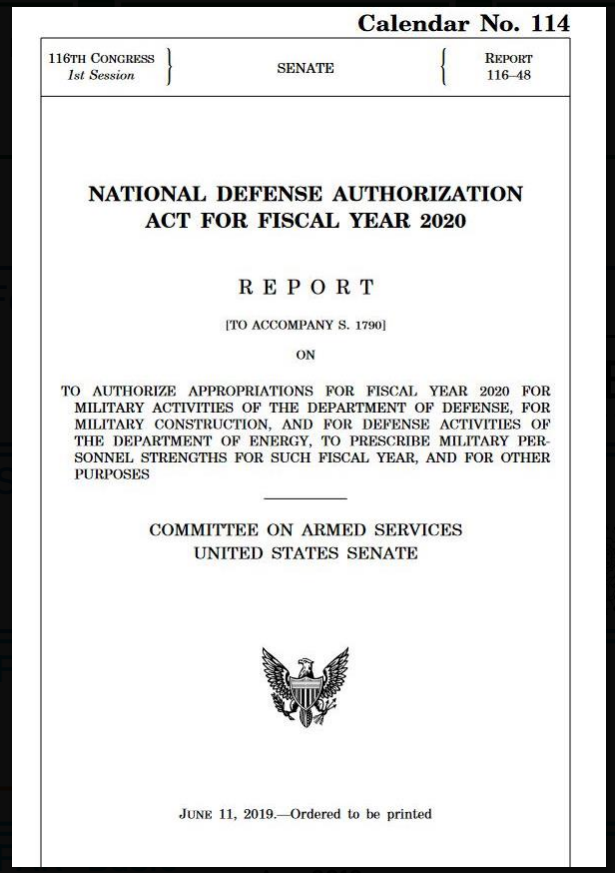
FAR "Basic"

Aug 2012 — Proposed Rule FAR Case 2011-020

Jun 2016 — Final Rule FAR Case 2011-020



A Timeline of Assumptions



Calendar No. 114

116TH CONGRESS *1st Session* | SENATE | REPORT 116–48

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2020

REPORT

[TO ACCOMPANY S. 1790]

ON

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2020 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE, FOR MILITARY CONSTRUCTION, AND FOR DEFENSE ACTIVITIES OF THE DEPARTMENT OF ENERGY, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

JUNE 11, 2019.—Ordered to be printed

> Currently, the Department of Defense mandates that defense contractors meet the requirements of NIST [SP] 800-171 but does not audit compliance to this standard.

The committee is concerned that prime contractors are not overseeing their subcontractors' compliance with these cybersecurity requirements through the entire supply chain and that the Department lacks access to information about its contractors' subcontractors.

The committee believes that prime contractors need to be held responsible and accountable for securing Department of Defense technology and sensitive information and for delivering products and capabilities that are uncompromised.

Developing a framework to enhance the cybersecurity of the defense industrial base will serve as an important first step toward securing the supply chain.

A Timeline of Assumptions

DFARS Rulemaking

Mar 2010 — ANPR DFARS Case 2008-D028

Jun 2011

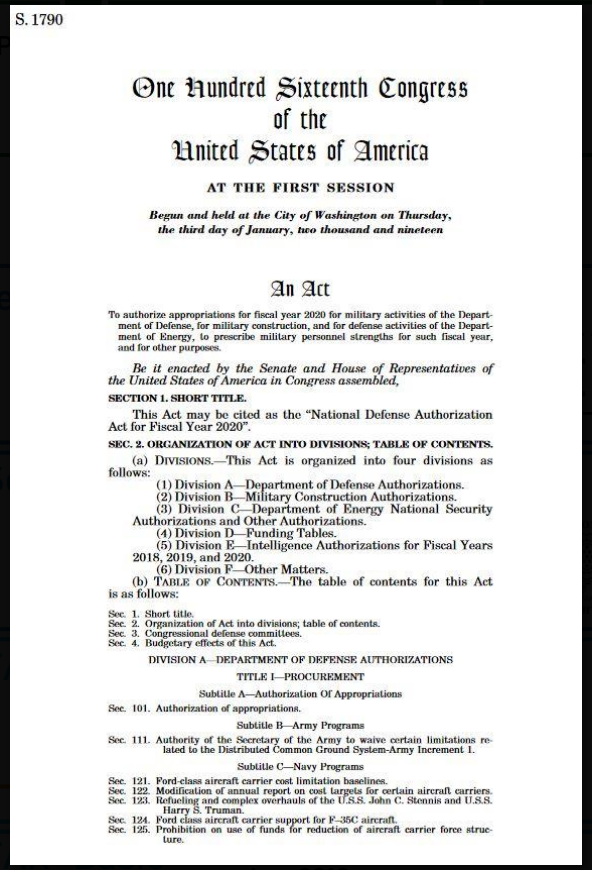
Nov 2013

Aug 2015 — Interim Rule DFARS Case 2013-D018

Dec 2015 — Interim Rule DFARS Case 2013-D018

Oct 2016 — Final Rule DFARS Case 2013-D018

Dec 2017 — NIST SP 800-171 Implementation Deadline



S. 1790

One Hundred Sixteenth Congress
of the
United States of America

AT THE FIRST SESSION

Begun and held at the City of Washington on Thursday, the third day of January, two thousand and nineteen

An Act

To authorize appropriations for fiscal year 2020 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Defense Authorization Act for Fiscal Year 2020".

SEC. 2. ORGANIZATION OF ACT INTO DIVISIONS; TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized into four divisions as follows:

(1) Division A—Department of Defense Authorizations.
(2) Division B—Military Construction Authorizations.
(3) Division C—Department of Energy National Security Authorizations and Other Authorizations.
(4) Division D—Funding Tables.
(5) Division E—Intelligence Authorizations for Fiscal Years 2018, 2019, and 2020.
(6) Division F—Other Matters.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title.
Sec. 2. Organization of Act into divisions; table of contents.
Sec. 3. Congressional defense committees.
Sec. 4. Budgetary effects of this Act.

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

Subtitle A—Authorization Of Appropriations

Sec. 101. Authorization of appropriations.

Subtitle B—Army Programs

Sec. 111. Authority of the Secretary of the Army to waive certain limitations related to the Distributed Common Ground System-Army Increment 1.

Subtitle C—Navy Programs

Sec. 121. Ford-class aircraft carrier cost limitation baselines.
Sec. 122. Modification of annual report on cost targets for certain aircraft carriers.
Sec. 123. Refueling and complex overhauls of the U.S.S. John C. Stennis and U.S.S. Harry S. Truman.
Sec. 124. Ford class aircraft carrier support for F–35C aircraft.
Sec. 125. Prohibition on use of funds for reduction of aircraft carrier force structure.

SEC. 1648

Framework to Enhance Cybersecurity of the United States Defense Industrial Base

The Secretary of Defense shall develop a consistent, comprehensive framework to enhance cybersecurity for the United States defense industrial base.

…to be imposed on the defense industrial base for the purpose of assessing the cybersecurity of individual contractors.

Nov 2010 — Executive Order 13556

Aug 2012 — Proposed Rule FAR Case 2011-020

Jun 2016 — Final Rule FAR Case 2011-020

Proposed Rule 32 CFR 2002

Final Rule 32 CFR 2002

SP 800-171 rev 1

DEFCERT

A Timeline of Assumptions

DFARS Rulemaking

Mar 2010 — ANPR DFARS Case 2008-D028

Jun 2011 — Proposed Rule DFARS Case 2011-D039

Nov 2013 — Final Rule DFARS Case 2011-D039

Aug 2015

Dec 2015

Oct 2016 — Final Rule DFARS Case 2013-D018

Dec 2017 — NIST SP 800-171 Implementation Deadline

1 Federal CUI Rule

ORGANIZATIONAL DE

Sep 2016 — Final Rule 32 CFR 2002

2 Security Requirements

Nov 2010 — Executive Order 13556

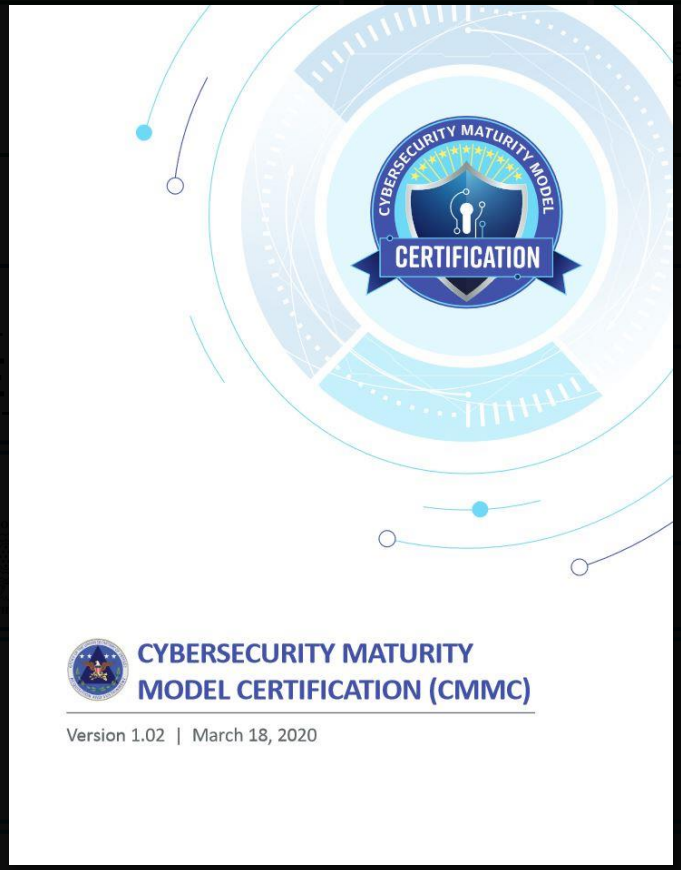
Dec 2016 — NIST SP 800-171 rev 1

3 FAR CUI Rule

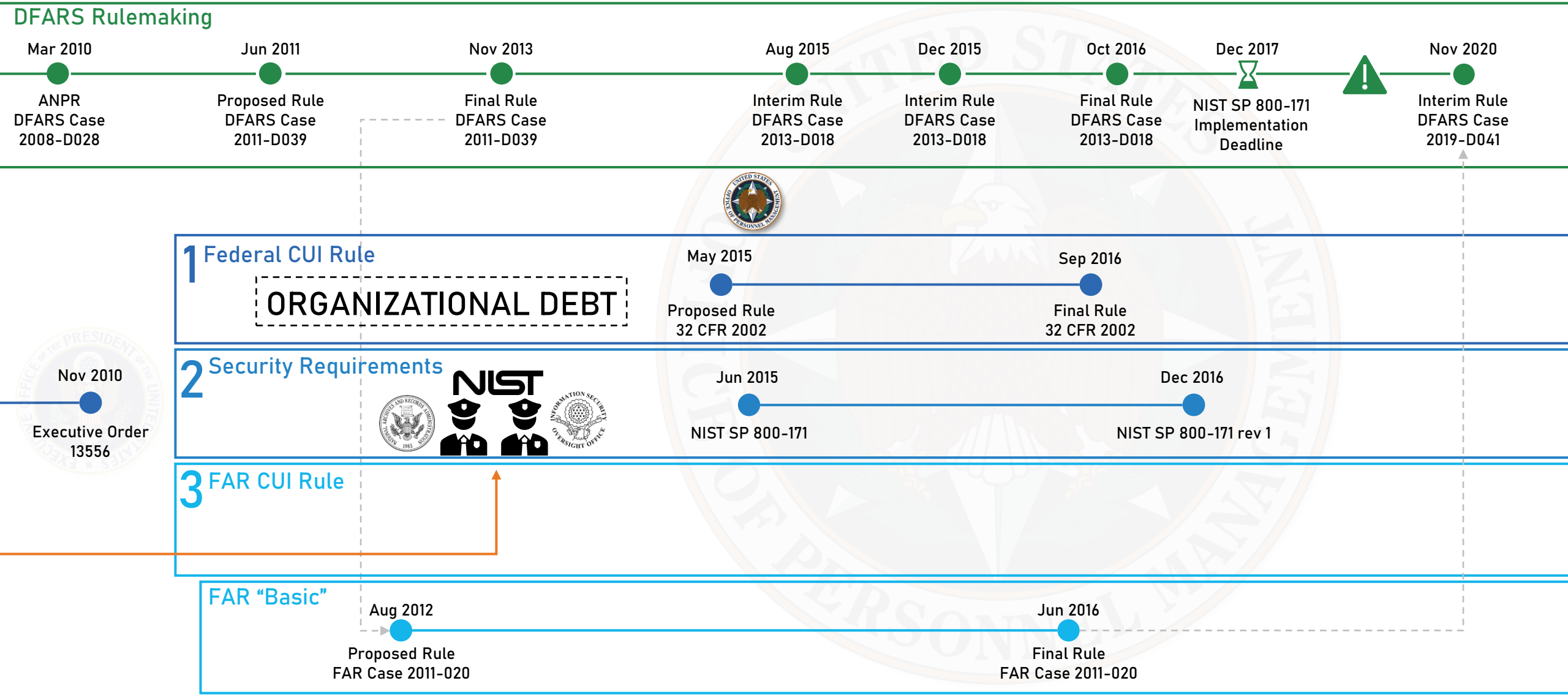
FAR "Basic"

Aug 2012 — Proposed Rule FAR Case 2011-020

Jun 2016 — Final Rule FAR Case 2011-020



A Timeline of Assumptions



DEFCERT

November 2020 – Interim Rule

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 Methodology

DFARS 252.204-7021 (Clause)

Cybersecurity Maturity Model Certification Requirements

Both Assumptions and Organizational Debt Accumulate

A contractor should already be aware of the security requirements they have not yet implemented and have documented plans of action for those requirements.

Burden associated with conducting a self-assessment is the time burden associated with calculating and uploading the score: 45 minutes, $74.31

DEFCERT

Source: DFARS Case 2019-D041

November 2020 – Interim Rule

	CMMC Level 1	CMMC Level 2	CMMC Level 3
Assessment	$2,999.56	$22,466.88	$51,095.60
Nonrecurring Engineering	N/A	$8,135.00	$26,214.00
Recurring Engineering	N/A	$20,154.00	$41,666.00
Estimated Total	$2,999.56	$50,755.88	$118,975.60

- 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.

- 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.

- 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

Source: DFARS Case 2019-D041

Chapter 5

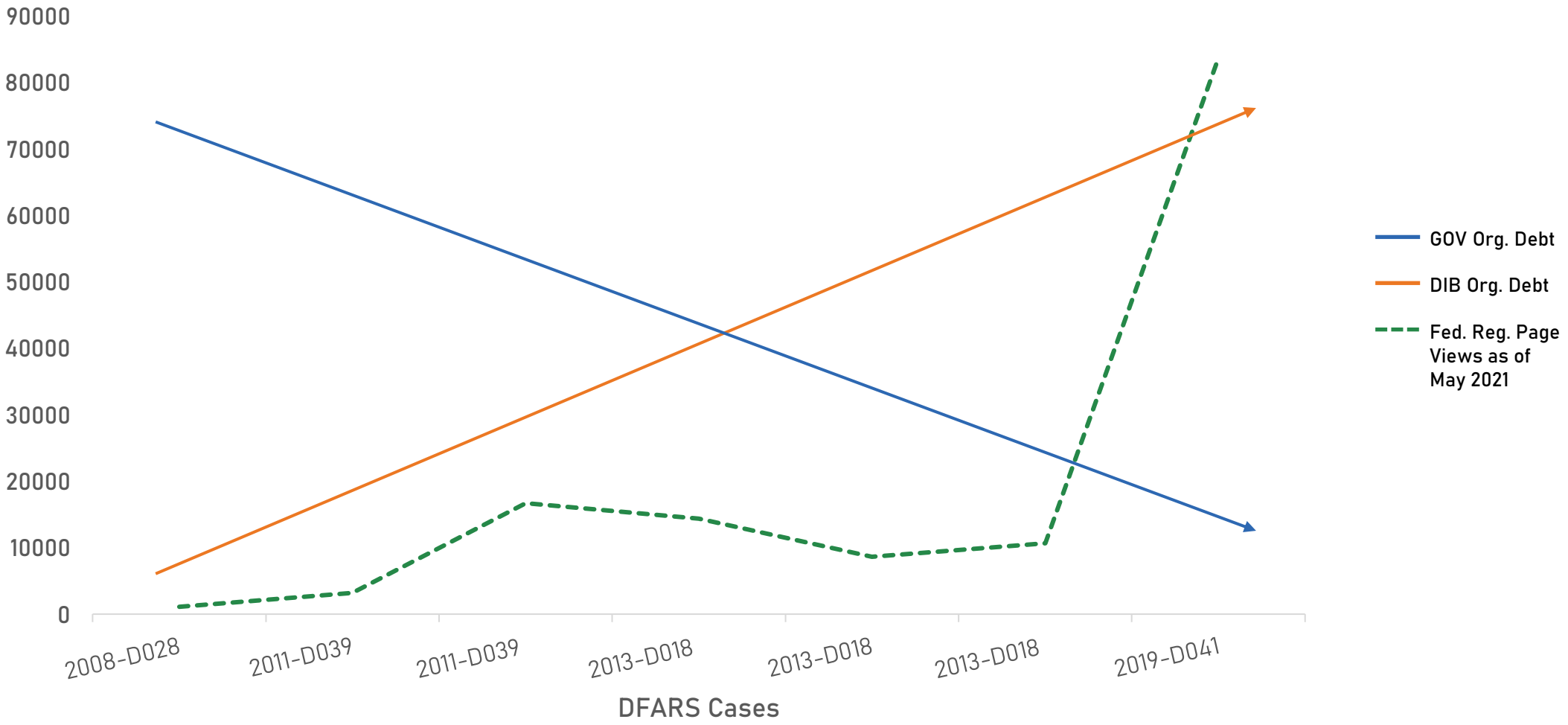
CMMC and the “Burden” Paradox

“How did you go bankrupt?” Bill asked.

“Two ways,” Mike said. *“Gradually, then suddenly.”*

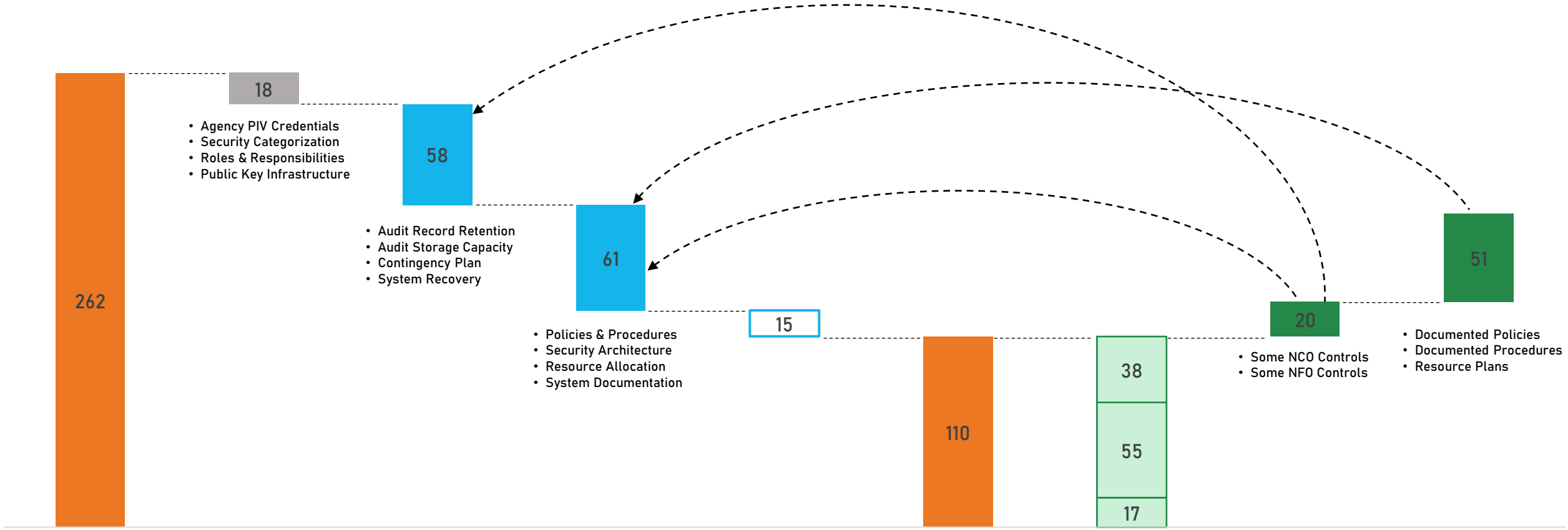
- Ernest Hemingway, *The Sun Also Rises*

Charting Organizational Debt (Notional)



DEFCERT

CMMC and the Paradox of Burden

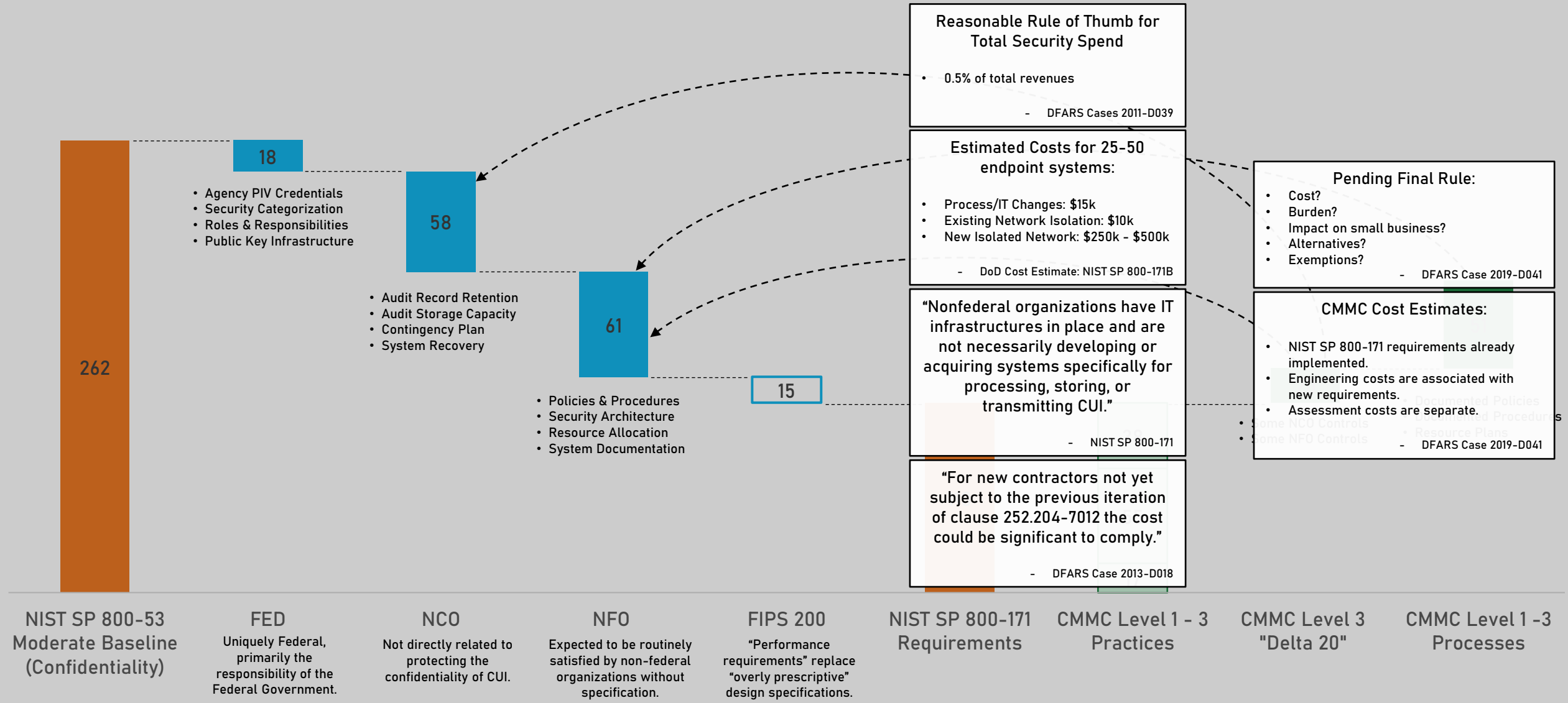


NIST SP 800-53 Moderate Baseline (Confidentiality)	FED	NCO	NFO	FIPS 200	NIST SP 800-171 Requirements	CMMC Level 1 - 3 Practices	CMMC Level 3 "Delta 20"	CMMC Level 1 -3 Processes
	Uniquely Federal, primarily the responsibility of the Federal Government.	Not directly related to protecting the confidentiality of CUI.	Expected to be routinely satisfied by non-federal organizations without specification.	"Performance requirements" replace "overly prescriptive" design specifications.				

DEFCERT

Sources: NIST SP 800-171 rev. 2 Appendix E; CMMC v1.02

CMMC and the Paradox of Burden



Sources: NIST SP 800-171 rev. 2 Appendix E; CMMC v1.02

Conclusion

Summary & Key Takeaways

“There are no solutions. There are only trade-offs.”

- Thomas Sowell

DEFCERT

Key Takeaways

1 CMMC Didn't Just Appear Out of the Blue

- CMMC isn't the forest. It's the leaves on a single tree.
- CMMC isn't going away.
- NIST SP 800-171 verification will exist, regardless of what it's called.
- Even if it did, the systemic burden that has accumulated over the years remains.

2 The Timeline Won't Stop With the Upcoming Final Rule

- The timeline is accelerating. There will be more rulemaking.
- SOLARWINDS is the new OPM.
- Upcoming Biden Executive Order on software supply chain security.
- Zero Trust Architecture.

3 We Already Know What the Upcoming Final Rule Will Say

- Almost every argument being made against DFARS, NIST SP 800-171, CMMC, and the CUI program has already been made and addressed in the Federal Register via formal rulemaking.
- Just because an argument may be sound and valid (cost, burden, small business impact, etc.) doesn't mean that it will win the debate.
- The cybersecurity arms race has eclipsed national security: the debate much more complex than it was 10 years ago.

4 Organizational Debt is the Enemy

- Organizational debt accumulates as it is never the top priority, until it's suddenly the only priority.
- There is a limit to how much technology can help.
- The majority of NIST SP 800-171 and CMMC requirements are non-technical.
- Relying on technology to solve non-technology problems is expensive and inefficient.
- Be skeptical of anyone promising suspiciously high compliance percentages as a result of "turn-key", silver bullet solutions.

5 The Burden of DFARS Cybersecurity Compliance is a Paradox

- Aggressive attempts to create a minimal viable security baseline inadvertently made compliance much more difficult for those companies with low security maturity.
- Poor assumptions in the design of NIST SP 800-171 does not magically delete the categorization and subsequent requirements to protect CUI.
- Counterintuitively, CMMC provides the exact mechanism for "reducing" burden: directly requiring things that were previously assumed to exist.

6 The Government is Still Burning Down it's Organizational Debt

- Upcoming Final DFARS Rule.
    - Anticipated momentarily.
- Upcoming FAR CUI Rule.
    - Anticipated Summer 2021.
- Agency CUI Program Implementation.
    - Anticipated December 2021.

DEFCERT

COMPLIANCE IN CONTEXT

info@defcert.com
www.defcert.com