Cybersecurity Policy Landscape

US Government

Executive

- EO Cyber 14028
- EO Supply Chain Review
- National Cyber Strategy
- Technology Memos

Legislative

- NDAA(s) & FY25
- 889B & Prohibitions
- Resolutions & Bills

Judicial

- Reporting
- **False Claims Act**

Regulatory

- DFARS CUI/CDI/CTI
  - FAQs/DoD Websites
  - **Safeguarding & Reporting (Rule 7012)**
  - DCMA Assessments/Score (Rule 7020)
  - CMMC 2.0 (Rule 7021 09/2025)
- FAR (Govt)
  - Basic Cyber
  - **NARA CUI Pending**
  - Incident/Threat
  - **Part 40 Supply Chain, SW, Security**
- Other(s)
  - ITAR/EAR
  - Sector Regulations; CIRCIA

Standards

NIST

Nonfederal

- **800-171**
- **800-171A**
- 800-172
- 800-172A
- Cyber Security Framework

Federal

- 800-53, 53A, & 53B
- 800-161/218 Cyber Supply Chain Risk Mgmt; Software
- FIPS, Bulletins, Drafts, & Papers
- 800-37 Risk Mgmt Framework
- 800-63 IdAM

Administrative

- **SEC**
- **DOJ/FBI**
- FedRAMP
- **DHS CISA**
- National Security Advisor
- GAO
- OMB
- GSA
- National Cyber Director
- NARA CUI Program
  - Registry
  - ISOO Notices
  - Handbook/Guide(s)
- Cross/Agency Task Force(s)

International

Standardizations

- ISO/IEC Standards
- (AU) Evaluation Program
- (CA) Protected B
- (UK) Cyber Essentials, Essentials Plus, GDPR

•

•

•

Department of Defense

Services, Offices & Programs:

Technology/Services Specific

- DoD CUI Registry – USD (I&S)
- FedRAMP Moderate & "Equivalent"
- FedRAMP SaaS
- NSA/CYBERCOM
- Resiliency, AI, Semi-Conductor,

DoD Memorandums, Directives, Letters

- DoD I&S DOD Instruction DoDI 5200.48 CUI & DCSA Guidance
- DoDI 5230.24 Marking
- DoDI 5000.90 Cybersecurity for Acquisition…& Program Managers
- NISPOM/DD254s
- Statements of Work, Performance Work Statements, CDRLs, …

Approved for Public Release

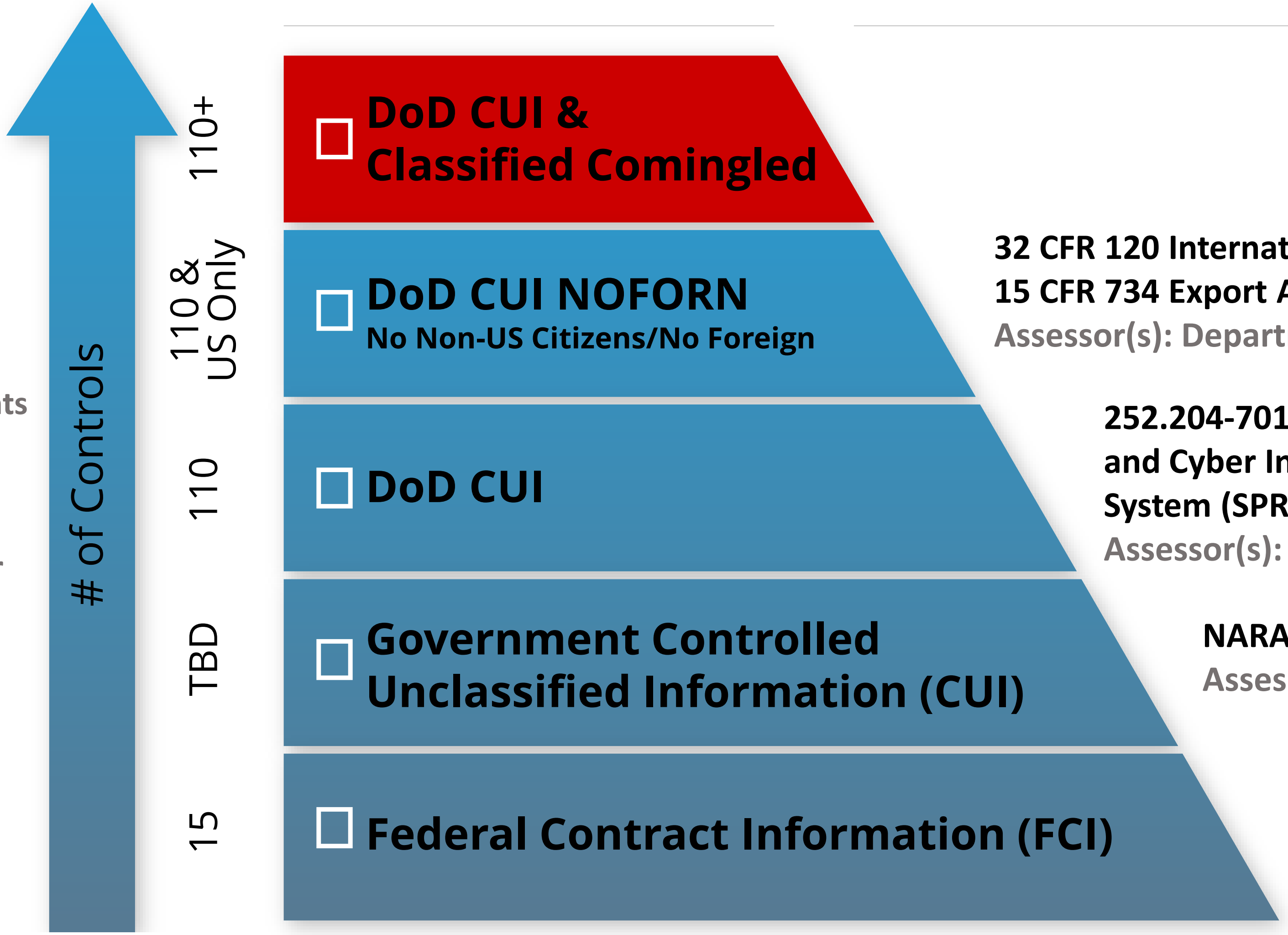
U.S. Government & DoD/DIB Sensitive Data Landscape - Summary

☑ Categorization

Authorities/Regulation/Contract Requirements

Additional Considerations:

- Contract Requirements
- Incident Reporting
- Award Fees
- Fines/Debar
- False Claims



□ **DoD CUI & Classified Comingled**

□ **DoD CUI NOFORN**
No Non-US Citizens/No Foreign

□ **DoD CUI**

□ **Government Controlled Unclassified Information (CUI)**

□ **Federal Contract Information (FCI)**

Security Requirements

32 CFR 120 International Traffic in Arms Regulations
15 CFR 734 Export Administration Regulations *EAR99 Exempt
Assessor(s): Department of State and/or Commerce & DIBCAC

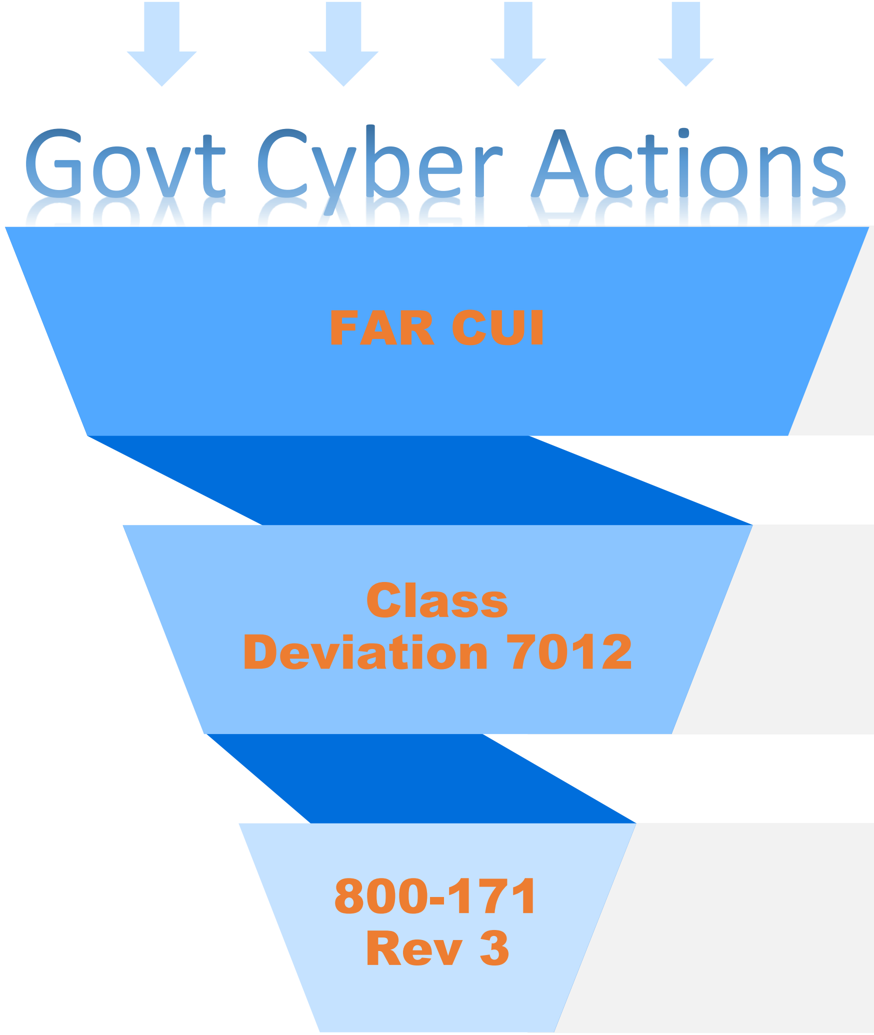
252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting & Supplier Performance Rating System (SPRS) 252.204-7020 NIST SP 800-171
Assessor(s): DoD DCMA DIBCAC or Future DoD CMMC C3PAO

NARA FAR Open Case 2017-016 CUI – *Pending*
Assessor(s): TBD Specified by each Agency’s Authority

52.204-21 Basic Safeguarding of Covered Contractor Information Systems
Assessor(s): Contract Agency Review(s)

Approved for Public Release

U.S. Govt Sensitive Information “Cascading” Items for 2024



Govt Cyber Actions

		Action	Impact	Timeline
FAR CUI	NARA	Public Comment	Potential to Simplify CUI	Rule 2Q24 Estimated
Class Deviation 7012	DoD	Sets DFARS 7012 to NIST 800-171 Rev 2	Dependent on Terms of Deviation	Issued 2 May 2024
800-171 Rev 3	NIST	Final Release of Rev 3	Initiate Gap Analysis & Use of POA&Ms	Published 14 May 2024 & 1 Year+

Absent Risk & Resiliency

Approved for Public Release

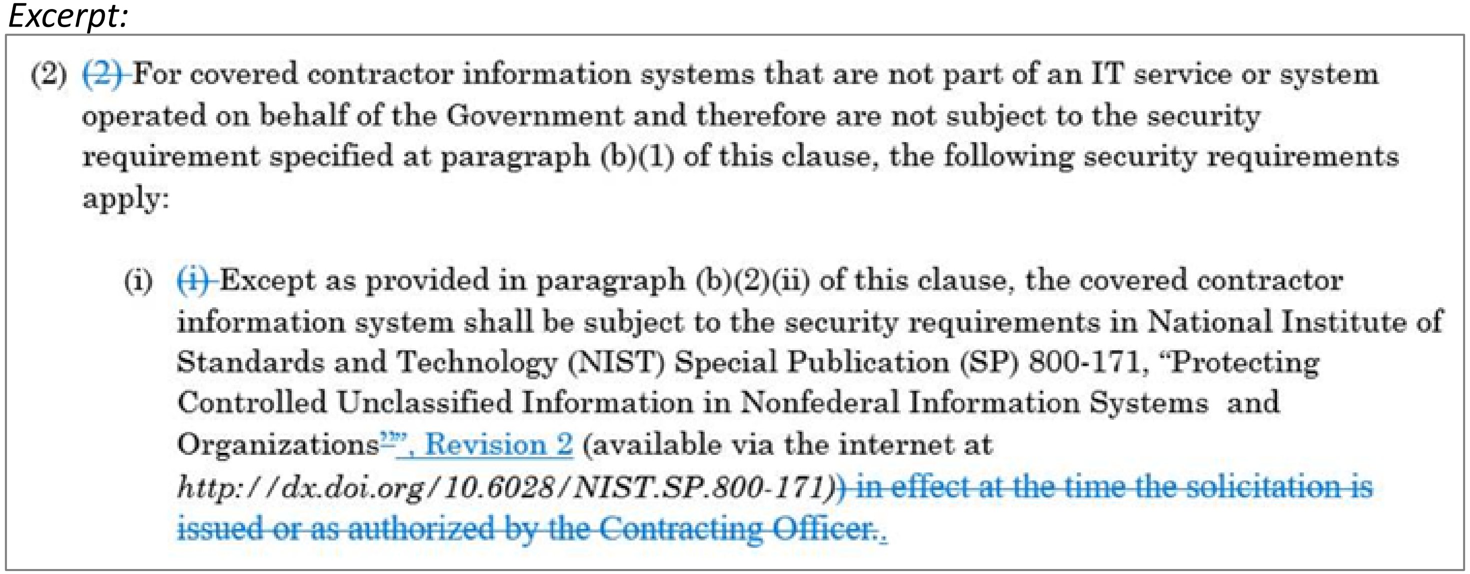
DoD Defense Pricing and Contracting (DPC) Issued Class Deviation on 2 May 2024

- **Verify Inclusion** https://www.acq.osd.mil/dpap/dars/class_deviations.html

Watch Items:

- **DoD has option to rescind at anytime**
  - **DFARS 7012 is being modified & in Rulemaking**
  - **NARA FAR CUI Imminent per DoD**
  - **CMMC Policy proposed rule specifies 800-171 Revision 2**
- **May require informing DoD Contracting Officers**

Excerpt:



(2) ~~(2)~~ For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) ~~(i)~~ Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations~~”~~”, Revision 2 (available via the internet at *http://dx.doi.org/10.6028/NIST.SP.800-171)*~~) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.~~.

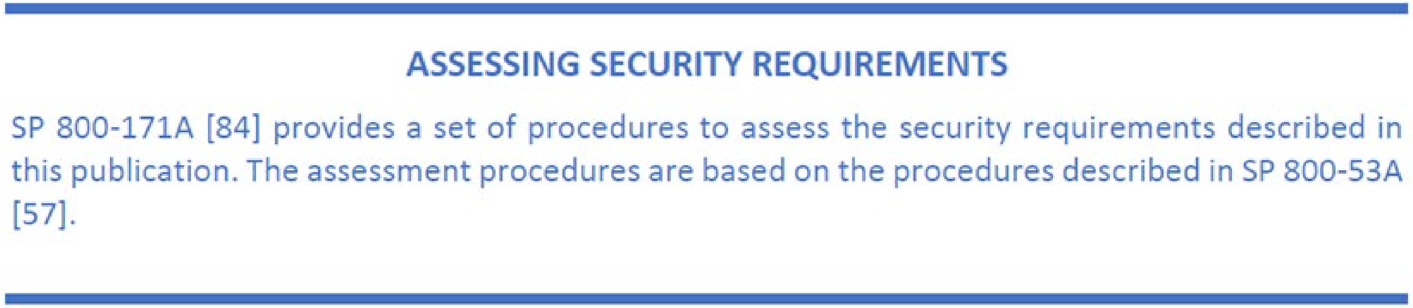
NARA FAR CUI - Pending

Implements the National Archives and Records Administration (NARA) Controlled Unclassified information (CUI) program of E.O. 13556, which provides implementing regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI.

05/20/2024 CAAC Chair sent draft proposed FAR rule to OIRA. OIRA reviewing.

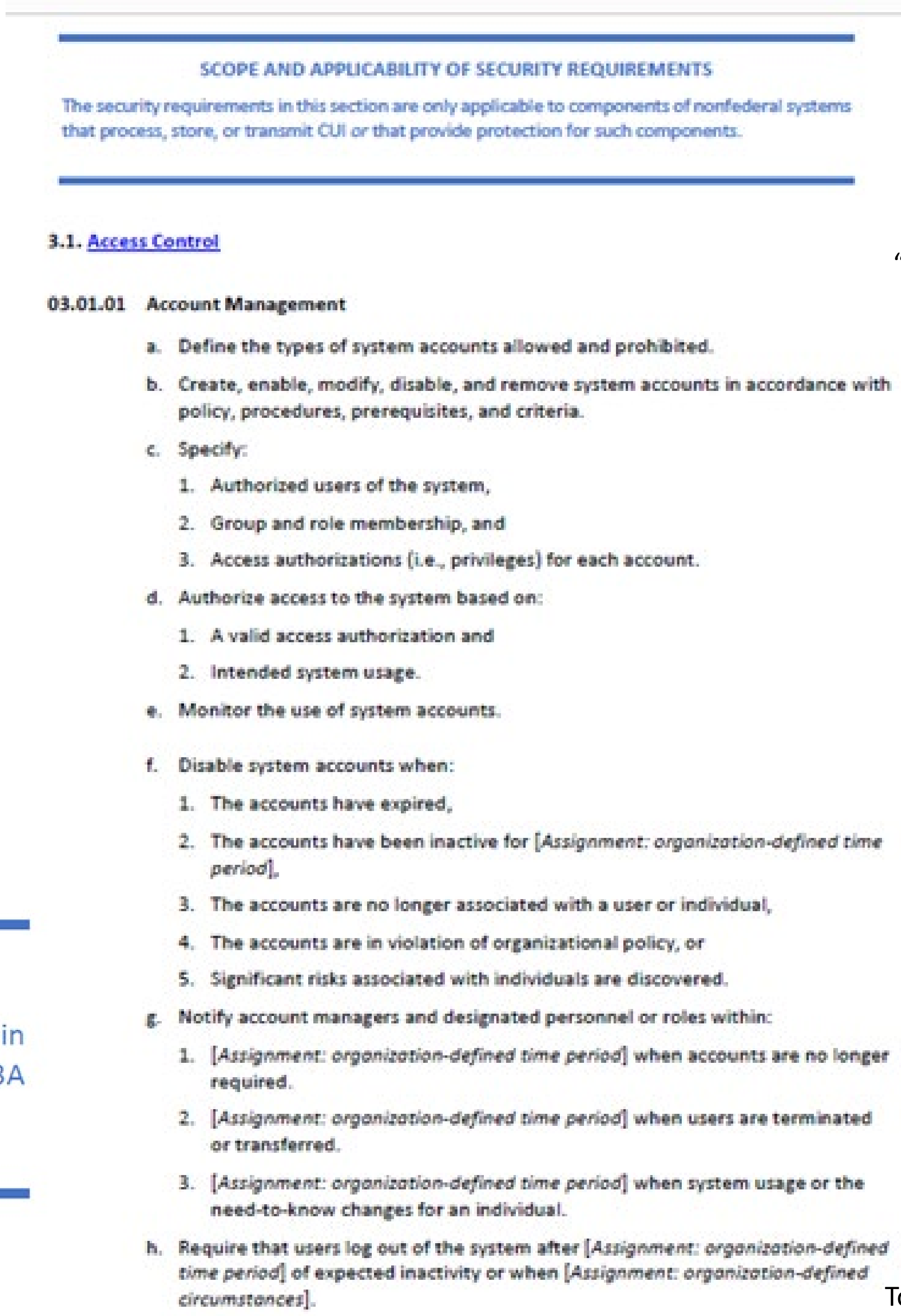
Approved for Public Release

- 110 pages, Format Change & no Change Management/Change Log
- Count of heading requirements from 110 to 97, however
  - Sub-requirements under review for “true” count
- Organization Defined Parameters (ODPs) have doubled in number from 40+ to 80+; contrary to public comments
- Term “Independent” removed from Audit and Review POA&Ms
  - Not directly related to protection of CUI (03.12.02 (b) 2)
- No change in Supply Chain Risk Management Family 03.17.01-03
  - Plan, Strategies, Tools, & Requirements and Processes
  - Excerpt: *Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements]*



ASSESSING SECURITY REQUIREMENTS

SP 800-171A [84] provides a set of procedures to assess the security requirements described in this publication. The assessment procedures are based on the procedures described in SP 800-53A [57].



SCOPE AND APPLICABILITY OF SECURITY REQUIREMENTS

The security requirements in this section are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components.

3.1. Access Control

“Action” Count:

03.01.01 Account Management

a. Define the types of system accounts allowed and prohibited. 2

b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria. 20

c. Specify:

1. Authorized users of the system, 1
2. Group and role membership, and 2
3. Access authorizations (i.e., privileges) for each account. 1

d. Authorize access to the system based on:

1. A valid access authorization and 1
2. Intended system usage. 1

e. Monitor the use of system accounts. 1

f. Disable system accounts when:

1. The accounts have expired, 1
2. The accounts have been inactive for [*Assignment: organization-defined time period*], 1
3. The accounts are no longer associated with a user or individual, 1
4. The accounts are in violation of organizational policy, or 1
5. Significant risks associated with individuals are discovered. 1

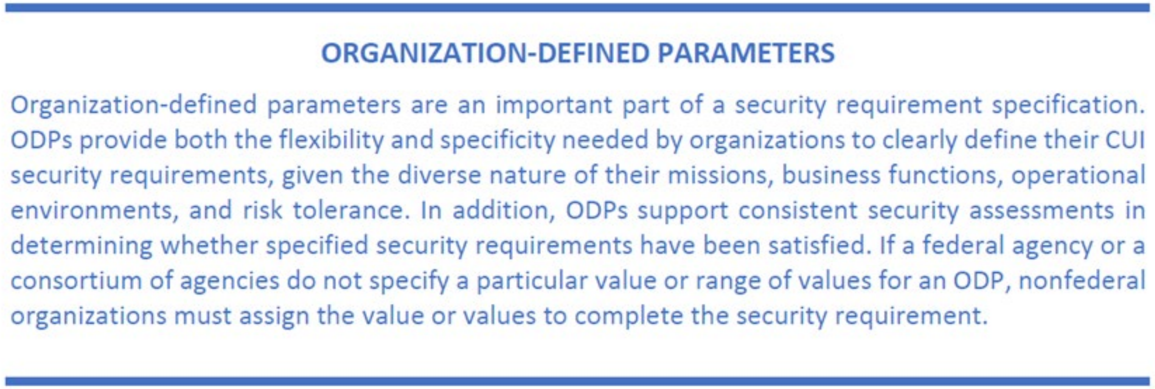
g. Notify account managers and designated personnel or roles within:

1. [*Assignment: organization-defined time period*] when accounts are no longer required. 1
2. [*Assignment: organization-defined time period*] when users are terminated or transferred. 4
3. [*Assignment: organization-defined time period*] when system usage or the need-to-know changes for an individual. 4

h. Require that users log out of the system after [*Assignment: organization-defined time period*] of expected inactivity or when [*Assignment: organization-defined circumstances*]. 2+

Total 45+

- Organization Defined Parameters (ODPs) have doubled in number from 40+ to 80+
  - Contrary to public comments to limit and request to clarify organization to the system owner (Company specified in place of Government Agency specified)
- Parameters may be expanded per the terms used:
  - Selection (one or more)
  - Circumstances
  - Functions
  - Events
  - Additional Actions
  - Configuration Settings
  - … variations are exponential



ORGANIZATION-DEFINED PARAMETERS

Organization-defined parameters are an important part of a security requirement specification. ODPs provide both the flexibility and specificity needed by organizations to clearly define their CUI security requirements, given the diverse nature of their missions, business functions, operational environments, and risk tolerance. In addition, ODPs support consistent security assessments in determining whether specified security requirements have been satisfied. If a federal agency or a consortium of agencies do not specify a particular value or range of values for an ODP, nonfederal organizations must assign the value or values to complete the security requirement.

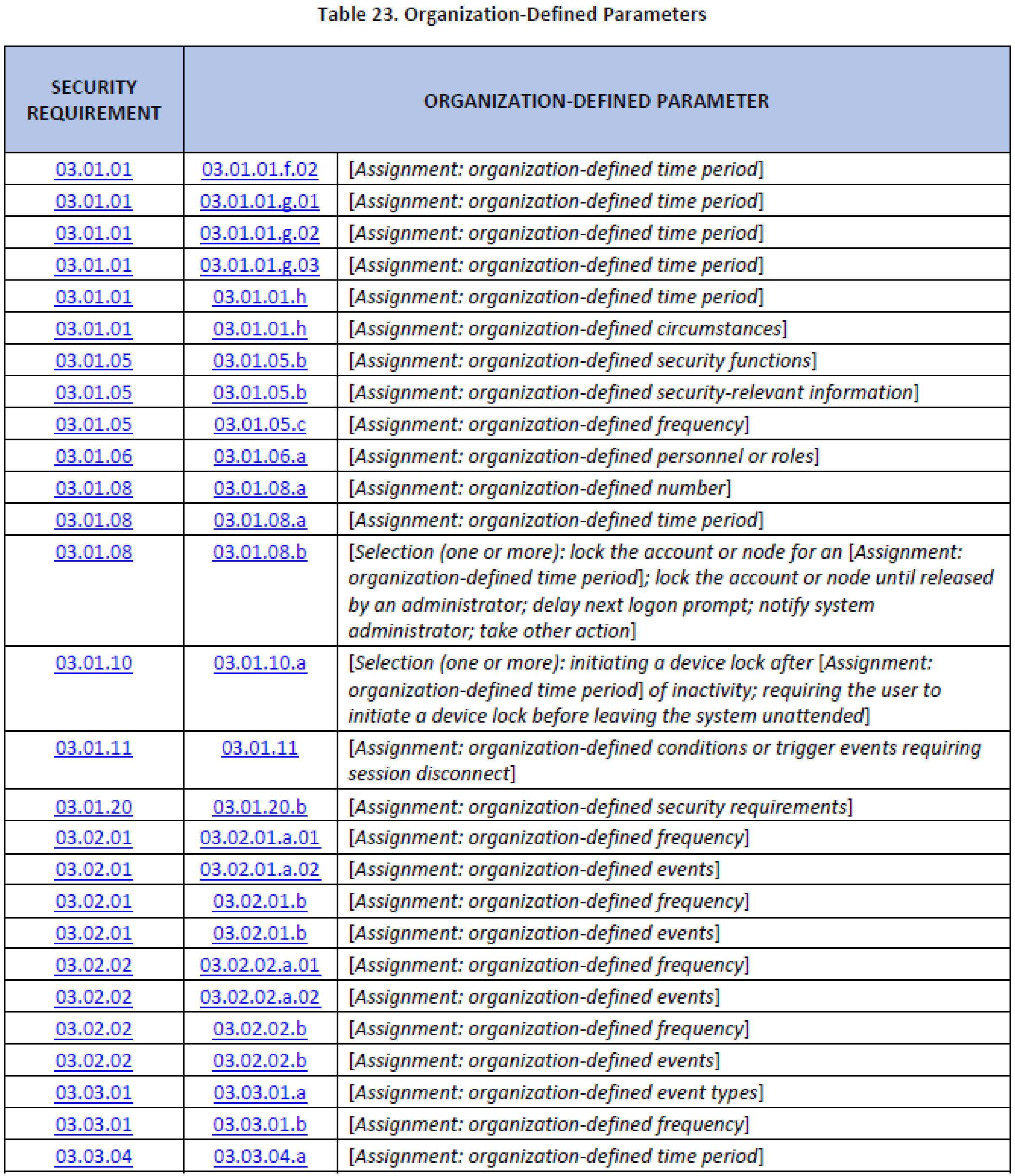


Table 23. Organization-Defined Parameters

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.01.01	03.01.01.f.02	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.g.01	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.g.02	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.g.03	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.h	[*Assignment: organization-defined time period*]
03.01.01	03.01.01.h	[*Assignment: organization-defined circumstances*]
03.01.05	03.01.05.b	[*Assignment: organization-defined security functions*]
03.01.05	03.01.05.b	[*Assignment: organization-defined security-relevant information*]
03.01.05	03.01.05.c	[*Assignment: organization-defined frequency*]
03.01.06	03.01.06.a	[*Assignment: organization-defined personnel or roles*]
03.01.08	03.01.08.a	[*Assignment: organization-defined number*]
03.01.08	03.01.08.a	[*Assignment: organization-defined time period*]
03.01.08	03.01.08.b	[*Selection (one or more): lock the account or node for an* [*Assignment: organization-defined time period*]*; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action*]
03.01.10	03.01.10.a	[*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*]
03.01.11	03.01.11	[*Assignment: organization-defined conditions or trigger events requiring session disconnect*]
03.01.20	03.01.20.b	[*Assignment: organization-defined security requirements*]
03.02.01	03.02.01.a.01	[*Assignment: organization-defined frequency*]
03.02.01	03.02.01.a.02	[*Assignment: organization-defined events*]
03.02.01	03.02.01.b	[*Assignment: organization-defined frequency*]
03.02.01	03.02.01.b	[*Assignment: organization-defined events*]
03.02.02	03.02.02.a.01	[*Assignment: organization-defined frequency*]
03.02.02	03.02.02.a.02	[*Assignment: organization-defined events*]
03.02.02	03.02.02.b	[*Assignment: organization-defined frequency*]
03.02.02	03.02.02.b	[*Assignment: organization-defined events*]
03.03.01	03.03.01.a	[*Assignment: organization-defined event types*]
03.03.01	03.03.01.b	[*Assignment: organization-defined frequency*]
03.03.04	03.03.04.a	[*Assignment: organization-defined time period*]

Notional DoD CMMC Timeline

DoD Policy Pending

32 Code of Federal Regulations (CFR)

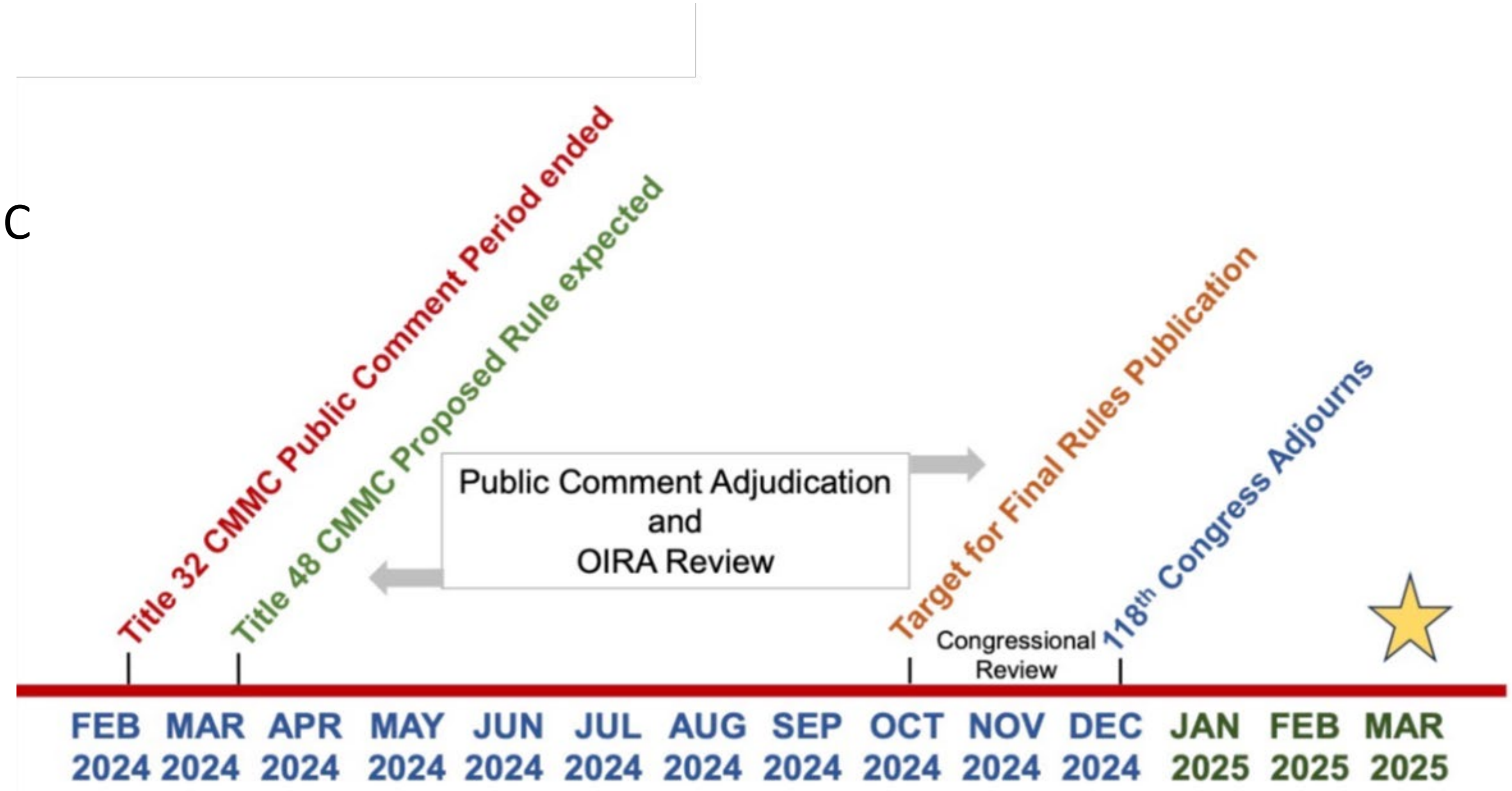
Authorizes the DoD to implement the CMMC program, framework and components

- The proposed rule was published Dec 2023 & public comments provided
- DoD adjudication of comments in process

DoD Requirements Pending

48 CFR DFARS 252.204-7021

Establishes the requirements for incorporating CMMC into DoD contracts



CMMC – Cybersecurity Maturity Model Certification
OIRA – White House Office of Information Regulatory Affairs

Source: NCMS

Approved for Public Release

National Defense Authorization Act (NDAA) FY25 - Status

350+ Amendment Provisions filed

House

- HR 8070 Week of June 10th for House Floor
- House Cyber, Information Technologies, and Innovation Subcommittee
  - AI, Quantum, Mobile Device
  - Volunteer/Free Cyber Experts, Rotational Assignments
  - DoD ATO Streamline

Cyber Subcomittee Excerpt:
DOD Defense Innovation Unit's available scientific and engineering positions, from five to 35, and allow five positions to be paid at 150 percent of the maximum rate

Senate

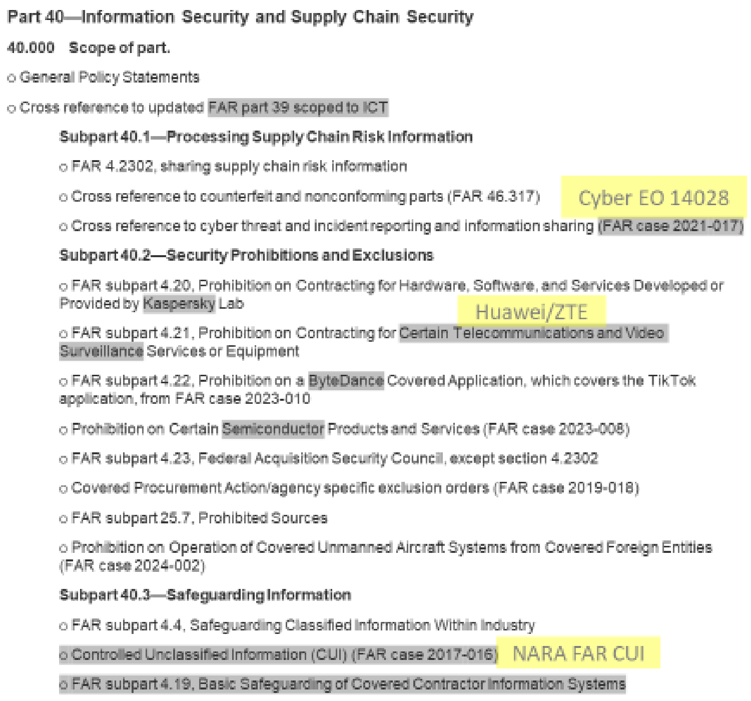
- $55B increase from 3% to 5% GDP
- Senate Armed Services Committee debate June 11th

FAR Part 40 Status

RFI on FAR Part 40 published on 9 April 2024
Responses due 10 June 2024

DoD, GSA, and NASA are providing an opportunity to provide comments on the **proposed** scope of FAR part 40

> *"Feedback provided should support the goal of providing a single location to cover broad security requirements that apply across acquisitions.*
>
> *Providing the acquisition team with a single, consolidated location in the FAR that addresses their role in implementing requirements related to managing information security and supply chain security when acquiring products and services."*



Part 40—Information Security and Supply Chain Security

40.000 Scope of part.

○ General Policy Statements

○ Cross reference to updated FAR part 39 scoped to ICT

Subpart 40.1—Processing Supply Chain Risk Information

○ FAR 4.2302, sharing supply chain risk information

○ Cross reference to counterfeit and nonconforming parts (FAR 46.317)

Cyber EO 14028

○ Cross reference to cyber threat and incident reporting and information sharing (FAR case 2021-017)

Subpart 40.2—Security Prohibitions and Exclusions

○ FAR subpart 4.20, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab

Huawei/ZTE

○ FAR subpart 4.21, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

○ FAR subpart 4.22, Prohibition on a ByteDance Covered Application, which covers the TikTok application, from FAR case 2023-010

○ Prohibition on Certain Semiconductor Products and Services (FAR case 2023-008)

○ FAR subpart 4.23, Federal Acquisition Security Council, except section 4.2302

○ Covered Procurement Action/agency specific exclusion orders (FAR case 2019-018)

○ FAR subpart 25.7, Prohibited Sources

○ Prohibition on Operation of Covered Unmanned Aircraft Systems from Covered Foreign Entities (FAR case 2024-002)

Subpart 40.3—Safeguarding Information

○ FAR subpart 4.4, Safeguarding Classified Information Within Industry

○ Controlled Unclassified Information (CUI) (FAR case 2017-016) NARA FAR CUI

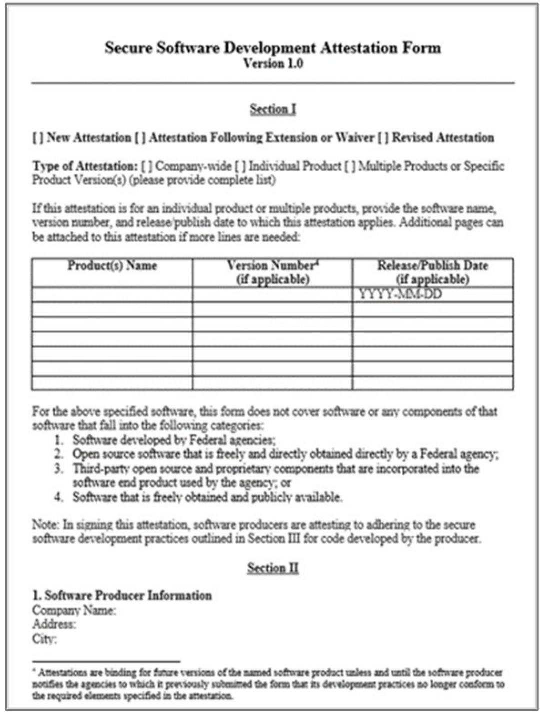
○ FAR subpart 4.19, Basic Safeguarding of Covered Contractor Information Systems

New FAR Part 40 titled "Information Security and Supply Chain Security"

Directives and/or Frameworks Individual & Specific initially to Critical Infrastructure Sectors -

- Communications
- Information Technology
- Financial Services
- Healthcare
- Transportation
- Maritime

Approved for Public Release



Secure Software Development Attestation Form
Version 1.0

Section I

[ ] New Attestation [ ] Attestation Following Extension or Waiver [ ] Revised Attestation

Type of Attestation: [ ] Company-wide [ ] Individual Product [ ] Multiple Products or Specific Product Version(s) (please provide complete list)

If this attestation is for an individual product or multiple products, provide the software name, version number, and release/publish date to which this attestation applies. Additional pages can be attached to this attestation if more lines are needed:

Product(s) Name	Version Number[4] (if applicable)	Release/Publish Date (if applicable)
		YYYY-MM-DD

For the above specified software, this form does not cover software or any components of that software that fall into the following categories:

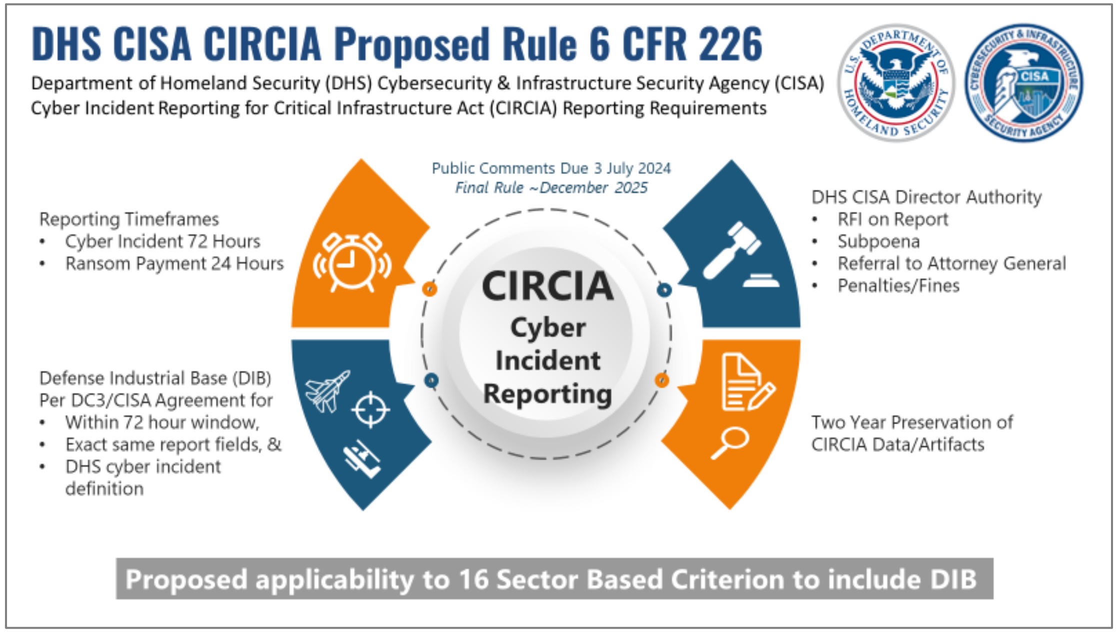
1. Software developed by Federal agencies;
2. Open source software that is freely and directly obtained directly by a Federal agency;
3. Third-party open source and proprietary components that are incorporated into the software end product used by the agency; or
4. Software that is freely obtained and publicly available.

Note: In signing this attestation, software producers are attesting to adhering to the secure software development practices outlined in Section III for code developed by the producer.

Section II

1. Software Producer Information
Company Name:
Address:
City:

[4] Attestations are binding for future versions of the named software product unless and until the software producer notifies the agencies to which it previously submitted the form that its development practices no longer conform to the required elements specified in the attestation.



DHS CISA CIRCIA Proposed Rule 6 CFR 226

Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA)
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

Public Comments Due 3 July 2024
Final Rule ~December 2025

CIRCIA Cyber Incident Reporting

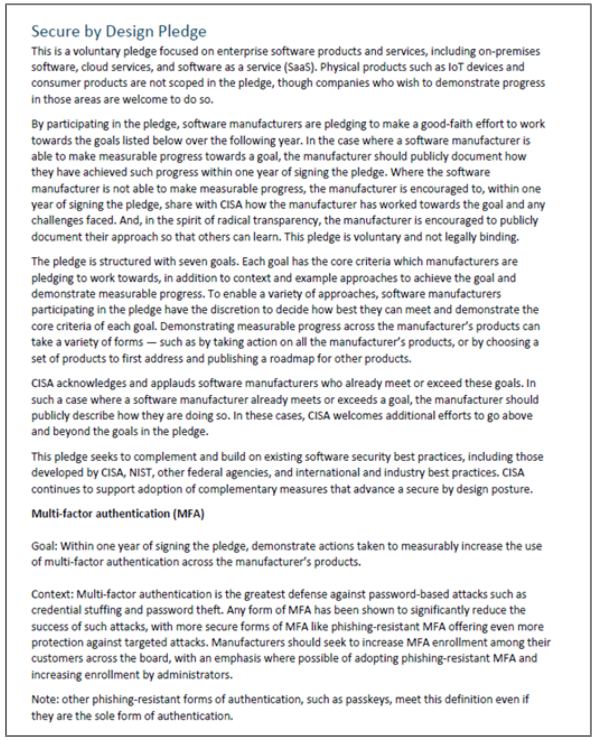
Reporting Timeframes
- Cyber Incident 72 Hours
- Ransom Payment 24 Hours

Defense Industrial Base (DIB) Per DC3/CISA Agreement for
- Within 72 hour window,
- Exact same report fields, &
- DHS cyber incident definition

DHS CISA Director Authority
- RFI on Report
- Subpoena
- Referral to Attorney General
- Penalties/Fines

Two Year Preservation of CIRCIA Data/Artifacts

Proposed applicability to 16 Sector Based Criterion to include DIB



Secure by Design Pledge

This is a voluntary pledge focused on enterprise software products and services, including on-premises software, cloud services, and software as a service (SaaS). Physical products such as IoT devices and consumer products are not scoped in the pledge, though companies who wish to demonstrate progress in those areas are welcome to do so.

By participating in the pledge, software manufacturers are pledging to make a good-faith effort to work towards the goals listed below over the following year. In the case where a software manufacturer is able to make measurable progress towards a goal, the manufacturer should publicly document how they have achieved such progress within one year of signing the pledge. Where the software manufacturer is not able to make measurable progress, the manufacturer is encouraged to, within one year of signing the pledge, share with CISA how the manufacturer has worked towards the goal and any challenges faced. And, in the spirit of radical transparency, the manufacturer is encouraged to publicly document their approach so that others can learn. This pledge is voluntary and not legally binding.

The pledge is structured with seven goals. Each goal has the core criteria which manufacturers are pledging to work towards, in addition to context and example approaches to achieve the goal and demonstrate measurable progress. To enable a variety of approaches, software manufacturers participating in the pledge have the discretion to decide how best they can meet and demonstrate the core criteria of each goal. Demonstrating measurable progress across the manufacturer's products can take a variety of forms — such as by taking action on all the manufacturer's products, or by choosing a set of products to first address and publishing a roadmap for other products.

CISA acknowledges and applauds software manufacturers who already meet or exceed these goals. In such a case where a software manufacturer already meets or exceeds a goal, the manufacturer should publicly describe how they are doing so. In these cases, CISA welcomes additional efforts to go above and beyond the goals in the pledge.

This pledge seeks to complement and build on existing software security best practices, including those developed by CISA, NIST, other federal agencies, and international and industry best practices. CISA continues to support adoption of complementary measures that advance a secure by design posture.

Multi-factor authentication (MFA)

Goal: Within one year of signing the pledge, demonstrate actions taken to measurably increase the use of multi-factor authentication across the manufacturer's products.

Context: Multi-factor authentication is the greatest defense against password-based attacks such as credential stuffing and password theft. Any form of MFA has been shown to significantly reduce the success of such attacks, with more secure forms of MFA like phishing-resistant MFA offering even more protection against targeted attacks. Manufacturers should seek to increase MFA enrollment among their customers across the board, with an emphasis where possible of adopting phishing-resistant MFA and increasing enrollment by administrators.

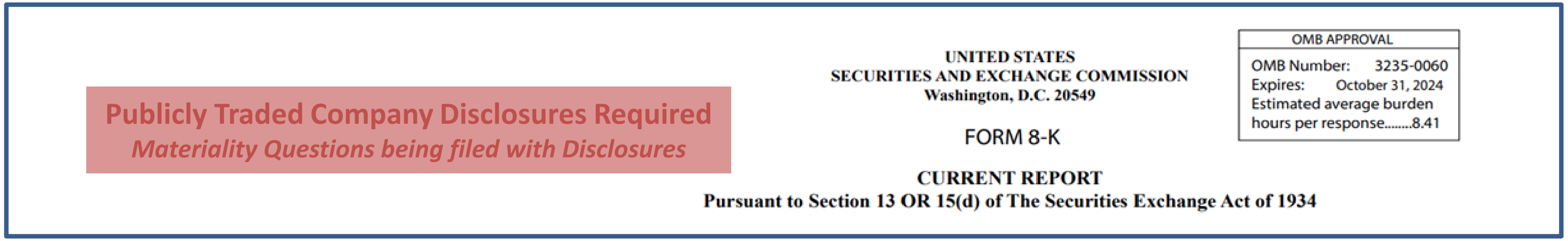
Note: other phishing-resistant forms of authentication, such as passkeys, meet this definition even if they are the sole form of authentication.

Open FAR Cases as of May 31, 2024

Case Number	Part Number	Title	Synopsis	Status
2023-002	1, 39, 52	Supply Chain Software Security	Implements section 4(n) of Executive Order 14028, which requires suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements.	05/30/2024 OMB identified draft proposed FAR rule issues. OFPP, FAR and DAR staff resolving issues.

Watch Items -
- **Repository for Federal IT**
- **Critical Software**
- **Legality of Licensed**
- **Risks & POA&M**
- **SBOM**

Securities & Exchange Commission



Publicly Traded Company Disclosures Required

Materiality Questions being filed with Disclosures

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

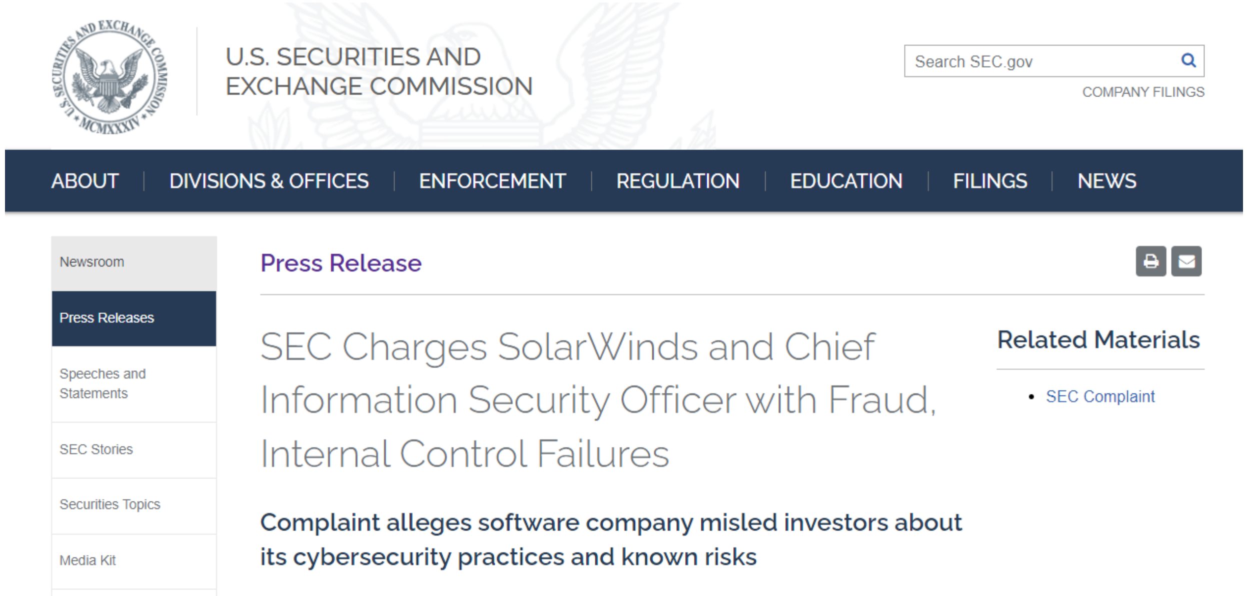
CURRENT REPORT
Pursuant to Section 13 OR 15(d) of The Securities Exchange Act of 1934

OMB APPROVAL	
OMB Number:	3235-0060
Expires:	October 31, 2024
Estimated average burden hours per response	8.41

Public companies to disclose both material cybersecurity incidents experienced and, on an annual basis, material information regarding cybersecurity risk management, strategy, and governance

SEC Erik Gerding Director, Division of Corporation Finance Statement on Materiality -
"encourage the filing of such voluntary disclosures in a manner that does not result in investor confusion or dilute the value of Item 1.05 disclosures regarding material cybersecurity incidents"

DoJ Matthew Olsen, Asst Attorney General for National Security – *"delayed companies' disclosures because making the attacks public would create substantial risks and raise national-security concerns"*



Press Release

SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

Complaint alleges software company misled investors about its cybersecurity practices and known risks

Related Materials

- SEC Complaint

Approved for Public Release

Cybersecurity Regulatory Landscape – Key Change

DFARS 7012 Class Deviation NIST 800-171 Rev 2

DoD issued Class Deviation on 2 May 2024 in anticipation of NIST 800-171 Rev 3 Release

Removes language at time of solicitation and specifies NIST 800-171 Rev 2

Immediately effective, communications and procedures pending

National Archives and Records Administration (NARA) FAR CUI

NARA has Agency Authority for Government CUI Program

Open FAR Case since 2017 with Govt Officials indicating pending release

Rule will “Simplify” CUI

NIST SP 800-161 Rev 1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

NIST

FAR Part 40 Supply Chain Risk Management

Consolidates multiple SCRM and C-SCRM best practices

Many controls require flow-down requirements to subs

Regulation(s) pending, FAR Part 40 RFI due 10 June 2024