



Cybersecurity Maturity Model Certification (CMMC)

US Cyber Security Requirements

Urban Lyxzén Bervelius
Security Compliance Officer, Saab Group



Released by DoD 28th of April 2022



DFARS

Change Number: DFARS Change 04/28/2022
Effective Date: 04/28/2022

Part 204

204.75

Section

SUBPART 204.75 —CYBERSECURITY MATURITY MODEL CERTIFICATION

Parent topic: [PART 204 - ADMINISTRATIVE AND INFORMATION MATTERS](#)

204.7500 Scope of subpart.

(a) This subpart prescribes policies and procedures for including the Cybersecurity Maturity Model Certification (CMMC) level requirements in DoD contracts. CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see <https://www.acq.osd.mil/cmmc/index.html>).

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.

204.7501 Policy.

(a) The contracting officer shall include in the solicitation the required CMMC level, if provided by the requiring activity. Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current (i.e., not more than 3 years old) CMMC certificate at the level required by the solicitation.

(b) Contractors are required to achieve, at time of award, a CMMC certificate at the level specified in the solicitation. Contractors are required to maintain a current (i.e., not more than 3 years old) CMMC certificate at the specified level, if required by the statement of work or requirement document, throughout the life of the contract, task order, or delivery order. Contracting officers shall not exercise an option period or extend the period of performance on a contract, task order, or delivery order, unless the contract has a current (i.e., not more than 3 years old) CMMC certificate at the level required by the contract, task order, or delivery order.

(c) The CMMC assessments shall not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a re-assessment may be necessary such as, but not limited to when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

204.7502 Procedures.

(a) When a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the contracting officer shall not—

(1) Award to an offeror that does not have a CMMC certificate at the level required by the solicitation; or

(2) Exercise an option or extend any period of performance on a contract, task order, or delivery order unless the contractor has a CMMC certificate at the level required by the contract.

(b) Contracting officers shall use Supplier Performance Risk System (SPRS) (<https://www.sprs.csd.disa.mil/>) to verify an offeror or contractor's CMMC level.

204.7503 Contract clause.

Use the clause at [252.204-7021](#), Cybersecurity Maturity Model Certification Requirements, as follows:

(a) Until September 30, 2025, in solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement a phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by OUSD(A&S).

(b) On or after October 1, 2025, in all solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items.

“(a) Until September 30, 2025, in solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement a phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by OUSD(A&S).”

“(b) On or after October 1, 2025, in all solicitations and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items.”

INTRODUCTION

US Government and Especially US Department of Defense (DoD) cybersecurity movement does not only affects the domestic industry, but also foreign entities because of their global supply chain.

The US defense industry base (DIB) is estimated to be more than 100 000.

The DoD global supply-chain is estimation by DoD to be more than 300 000.

DoD Estimate that 80 000 Suppliers will be required to have CMMC 2.0 L2 Capability

This is the reason for why the US Government cybersecurity movement impact companies abroad.

The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between \$57 billion and \$109 billion in 2016

[Source](#)

INTRODUCTION: WHY CMMC?

US is under cyber-attack by foreign adversaries, industry and criminals with the purpose to:

TECHNOLOGICAL ADVANTAGE

Protect and safeguard



Chinese hackers reveal "SEA DRAGON" – US Navy Supersonic Missile

U.S. authorities into a cyber event targeting U.S. nuclear facilities

China's New Comac C919 Jetliner Is Built With Stolen Technology

Russian hacking COVID-19 vaccine research

ONLINE DISINFORMATION IN THE UNITED STATES

INTRODUCTION: WHY CMMC?

US is under cyber-attack by foreign adversaries, industry and criminals with the purpose to:

- Exfiltration
- Disrupt critical infrastructure
- Obtain military superpower capability
- Disinformation (fake news)



INTRODUCTION: WHY CMMC?

“THE WEAKNESS LIES WITHIN SUPPLY CHAIN”

- WITH A PERFECT CASTLE, YOUR SUPPLY CHAIN WILL BE THE TARGET
- SMALL, MEDIUM BUSINESS
- COST, COMPETENCE AND LEGACY SYSTEM

“Attack him where he is unprepared, appear where you are not expected.”

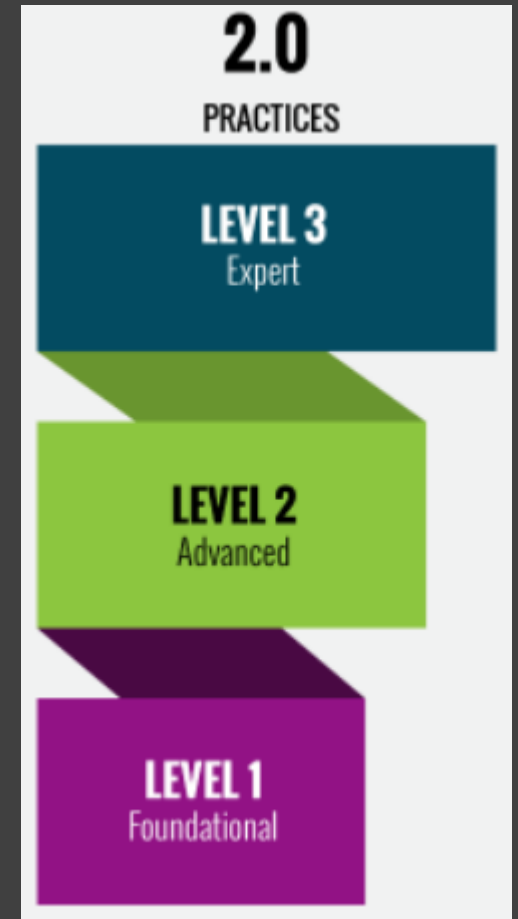
— Sun Tzu



[LINK TO MITRE REPORT](#)

CMMC 2.0: TRUST BUT VERIFY

- CMMC* IS A MATURITY MODEL DIVIDED INTO THREE LEVELS
 - LEVEL 1 = FEDERAL CONTRACT INFORMATION (FCI)
 - LEVEL 2 = CONTROLLED UNCLASSIFIED INFORMATION (CUI)
 - LEVEL 3 = ADVANCED PERSISTANT THREAT CAPABILITIES TO PROTECT OF CUI



[CMMC 2.0](#)

*Cybersecurity Maturity Model Certification

CMMC 2.0: TRUST BUT VERIFY

- CMMC IS A MATURITY MODEL IS DIVIDED INTO SELF ASSESSMENT AND THIRD PARTY ASSESSMENT
- SELF ASSESSMENT
 - LEVEL 1 (ALL CONTRACTS)
 - LEVEL 2 (VERY LIMITED NUMBER OF CONTRACTS)
- THIRD PART CERTIFICATION
 - LEVEL 2 (MAJORITY OF ALL CONTRACTS)
 - LEVEL 3 (VERY LIMITED NUMBER OF CONTRACTS)

[LINK TO MITRE REPORT](#)

WHO WILL BE SCOPED BY CMMC?

- ALL SUPPLIERS WILL BE SCOPED BY CMMC to be a in DoD supply chain
- CMMC LEVEL WILL BE STATED IN RFI/RFP
 - DFARS CLAUSE 252.204-7021
- ...meantime self assessment for Level 2 will appear
 - DFARS CLAUSE 252.204-7019 (Contractor)
 - DFARS CLAUSE 252.204-7020 (Flow-Down)



CONTROLLED
UNCLASSIFIED
INFORMATION

EXCEPTION

DoDI 5230.24, August 23, 2012

ENCLOSURE 3

PROCEDURES

1. All DoD Components generating or responsible for technical documents shall determine their distribution availability and mark them appropriately before primary distribution. Distribution statements shall be used in addition to applicable classification and dissemination control markings specified in Volume 2 of Reference (1).
2. DoD distribution statement markings shall not be required on technical proposals or similar documents submitted by contractors seeking DoD funds or contracts; however, markings prescribed by applicable acquisition regulations shall apply.

HOW TO IDENTIFY CUI: EXAMPLE



Identification and Marking of Covered Defense Information Preparation of Statement of Work (SOW)

Statement of Work (Section C)

- Prepared by Requiring Activity when DoD requires development and delivery of covered defense information

Contract Clauses (Section I), includes

- FAR Clause 52.204-2, when contract involves access to Confidential, Secret, or Top Secret information
- FAR Clause 52.204-21, when contract involves Federal Contract Information
- DFARS Clause 252.204-7012 in all contracts except COTS

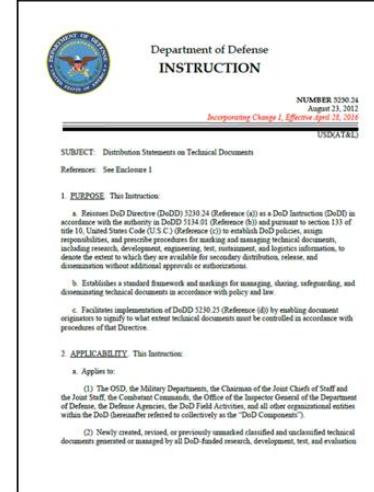
List of Attachments (Section J)

- Data deliverables as identified in Contract Data Requirements List (CDRL)
- Security Classification Guides
- Specifications
- Other Government Furnished Information

CONTRACT SECTION	PART I. THE SCHEDULE	
	A Solicitation/Contract Form	
	B Supplies or Services and Prices/Costs	
SOW	C Description/Specifications/Work Statement	
1. Scope	D Packaging and Marking	
2. Reference Doc.	E Inspection and Acceptance	
3. Requirements	F Deliveries or Performance	
	G Contract Administration Data	
Contract Delivery Dates	H Special Contract Requirements	Security Clearances Geographic Location Unique Requirements
CLINs		
Performance Time Frame		
	PART II. CONTRACT CLAUSES	
	I Contract Clauses	Clauses required by Procurement Regulations or Law which pertain to this Procurement
	PART III. LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS	
	J List of Attachments	List Contains: Security Form CDRL SOW Specification Financial Data: Sheet Exhibits
	PART IV. REPRESENTATIONS AND INSTRUCTIONS (Included in solicitations/RFPs only)	
Offeror's Type of Business	K Representations, certifications, and Other Statements of Offerors	Type of Contract, Solicitation Definitions, Prop reqmts, Progress Payments, etc.
Buy American Act Provisions	L Instructions, Conditions, and Notices to Offerors	
Cost Accounting Standards	M Evaluation Factors for Award	How Proposal will be Evaluated
Notices, etc.		
		Contract Attachments (i.e., SOW/SOO) Contract Exhibits (i.e., CDRLs)



Identification and Marking of Covered Defense Information Contract Data Requirements List (CDRL) – Form DD1423



Department of Defense
INSTRUCTION

NUMBER 5230.24
August 23, 2012
Revising Change 1, Effective April 26, 2014

SUBJECT: Distribution Statements on Technical Documents

References: See Enclosure 1

1. PURPOSE: This instruction:

a. Reinstates DoD Directive (DoDD) 5230.24 (Reference (R)) as a DoD Instruction (DoDI) in accordance with the authority in DoDD 5230.01 (Reference (R)) and pursuant to section 133 of title 10, United States Code (U.S.C.) (Reference (R)) to establish DoD policies, assign responsibilities, and prescribe procedures for marking and managing technical documents, including research, development, engineering, test, maintenance, and logistics information, to ensure the extent to which they are available for secondary distribution, release, and dissemination without additional approvals or substantiations.

b. Establishes a standard framework and markings for managing, sharing, safeguarding, and disseminating technical documents in accordance with policy and law.

c. Facilitates implementation of DoDD 5230.25 (Reference (R)) by enabling document managers to identify in what extent technical documents must be controlled in accordance with procedures of that Directive.

2. APPLICABILITY: This instruction:

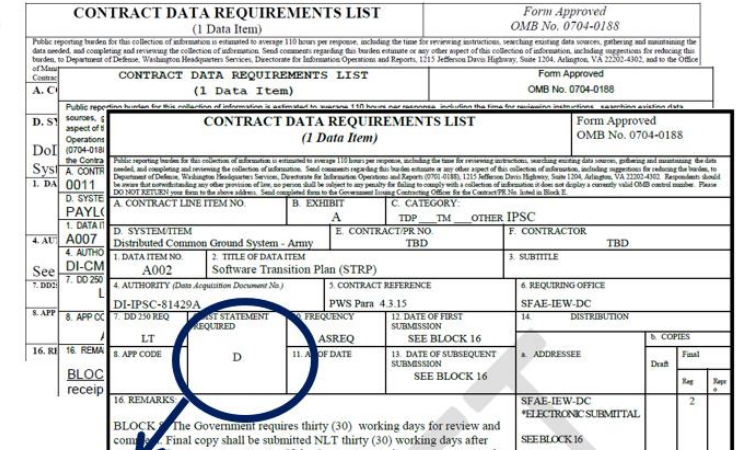
a. Applies to:

(1) The OSD, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Component");

(2) Newly created, revised, or previously unmarked classified and unclassified technical documents generated or managed by all DoD-funded research, development, test, and evaluation

DoDI 5230.24

No change to existing marking procedures for contract deliverables – e.g., controlled technical information is marked in accordance with DoDI 5230.24



CONTRACT DATA REQUIREMENTS LIST
(1 Data Item)

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 130 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Project (0704-0188).

CONTRACT DATA REQUIREMENTS LIST
(1 Data Item)

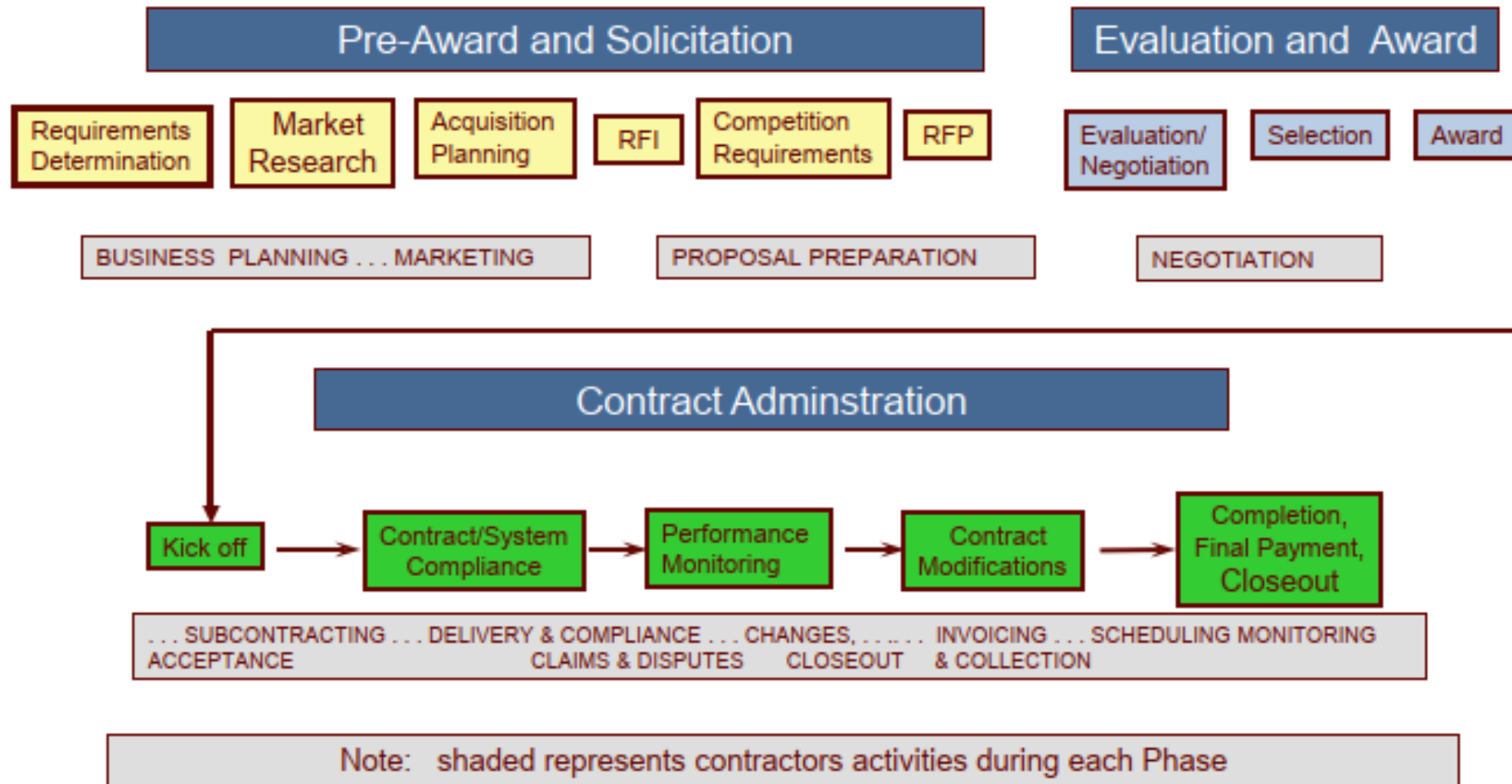
Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 130 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. Please DO NOT RETURN your form to the above address. Send completed forms to the Government Printing Office by the Contract PE No. listed in Block 5.

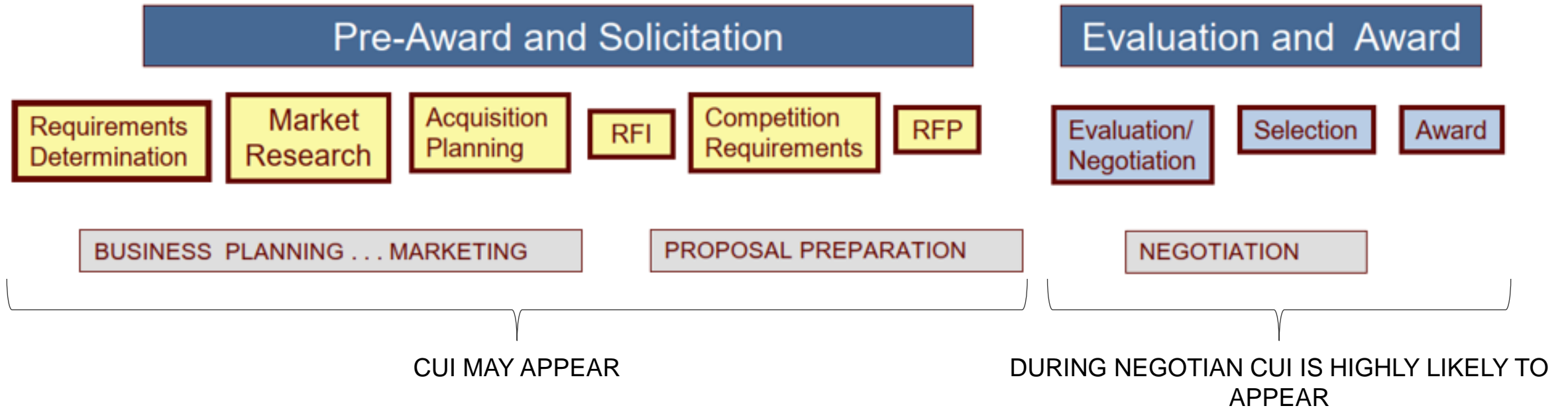
A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:	D. SYSTEM/ITEM	E. CONTRACT PR. NO.	F. CONTRACTOR
0011		TOP	Distributed Common Ground System - Army	TBD	TBD
1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE	4. AUTHORITY (Data Acquisition Document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
A002	Software Transition Plan (STRP)		DI-IPSC-81429A	PWS Para 4.3.15	SFAE-IEW-DC
7. DD 139 REQ. NO.	8. DD 139 REQ. STATEMENT REQUIRED	9. FREQUENCY	10. DATE OF FIRST SUBMISSION	11. DATE OF SUBSEQUENT SUBMISSION	12. DISTRIBUTION
		ASREQ		SEE BLOCK 16	
16. REMARKS	17. DATE OF SUBMISSION	18. DATE OF SUBSEQUENT SUBMISSION	19. ADDRESSSEE	20. COPIES	21. INITIALS
	SEE BLOCK 16	SEE BLOCK 16	SFAE-IEW-DC	*ELECTRONIC SUBMITTAL	
16. REMARKS: The Government requires thirty (30) working days for review and comment. Final copy shall be submitted NLT thirty (30) working days after					

Item 9. For technical information, specify requirement for contractor to mark the appropriate distribution statement on the data (ref. DoDI 5230.24); information is controlled when distribution statement is B-F

APPEARANCE OF CUI

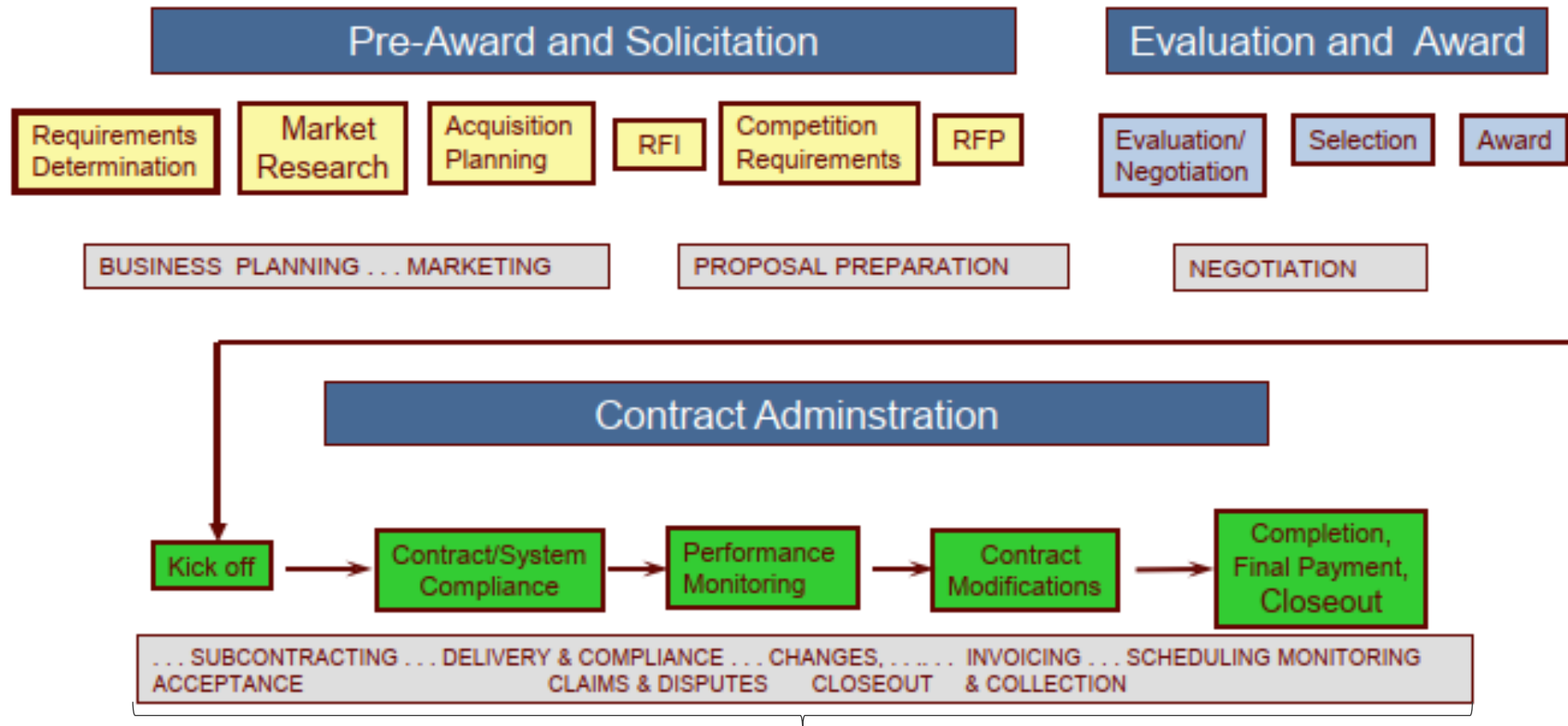


APPEARANCE OF CUI



Note: As long as no other communication have been made there is no requirement for the organization to protect its proposal as CUI

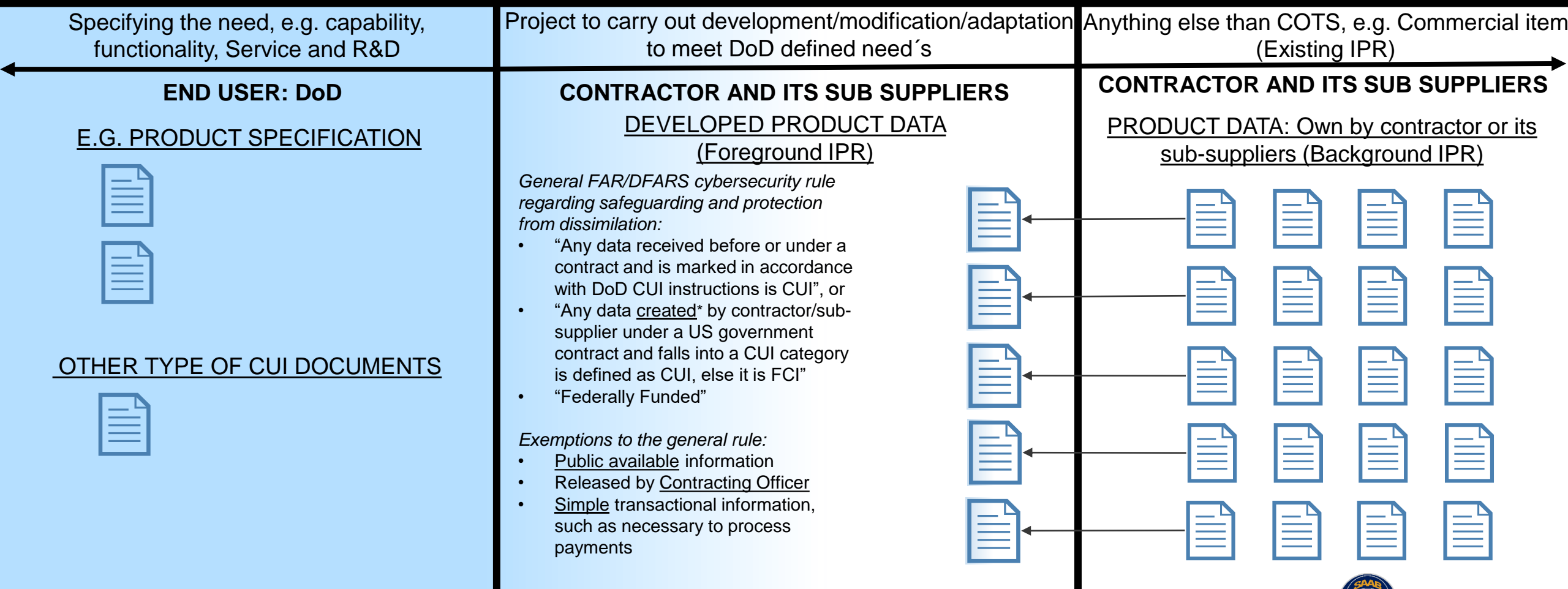
APPEARANCE OF CUI



FCI will appear but also CUI may appear as for example CTI and other CUI categories

CREATING CUI

Applicability of CUI framework



EXAMPLE CUI: VTESS CDRL



Home Search Data Bank Data Services Help



Contract Opportunity

General Information

Classification

Follow

Instrumentable Multiple Integrated Laser Engagement System Vehicle Tactical Engagement Simulation System (IMILES VTESS)

[Example of CDRL](#)

EXAMPLE CUI: VTESS CDRL

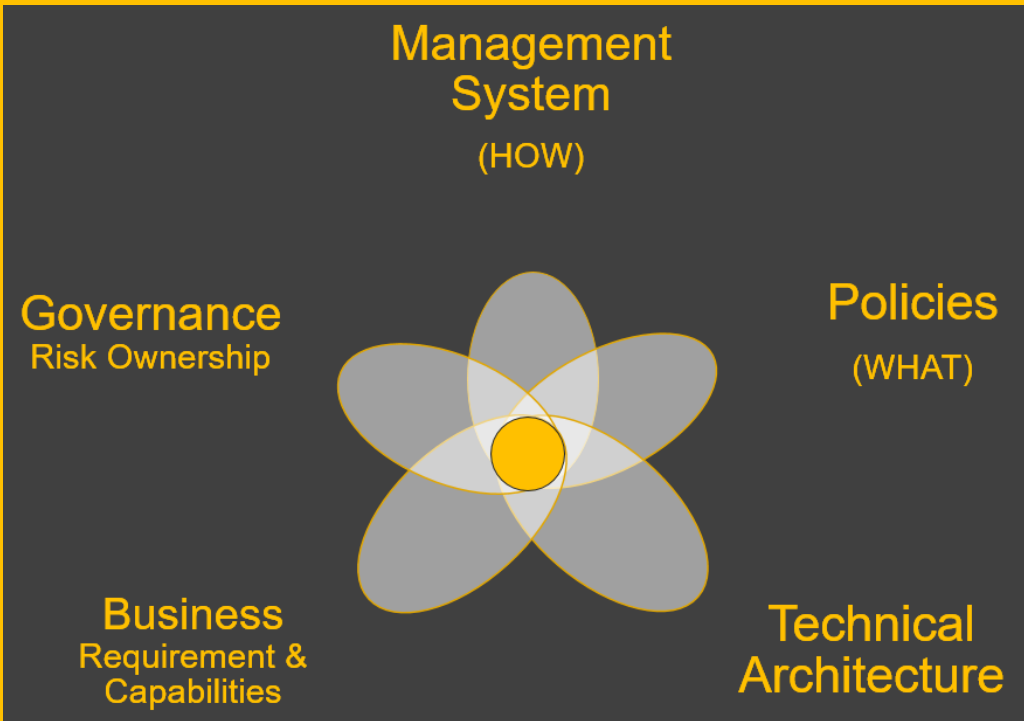
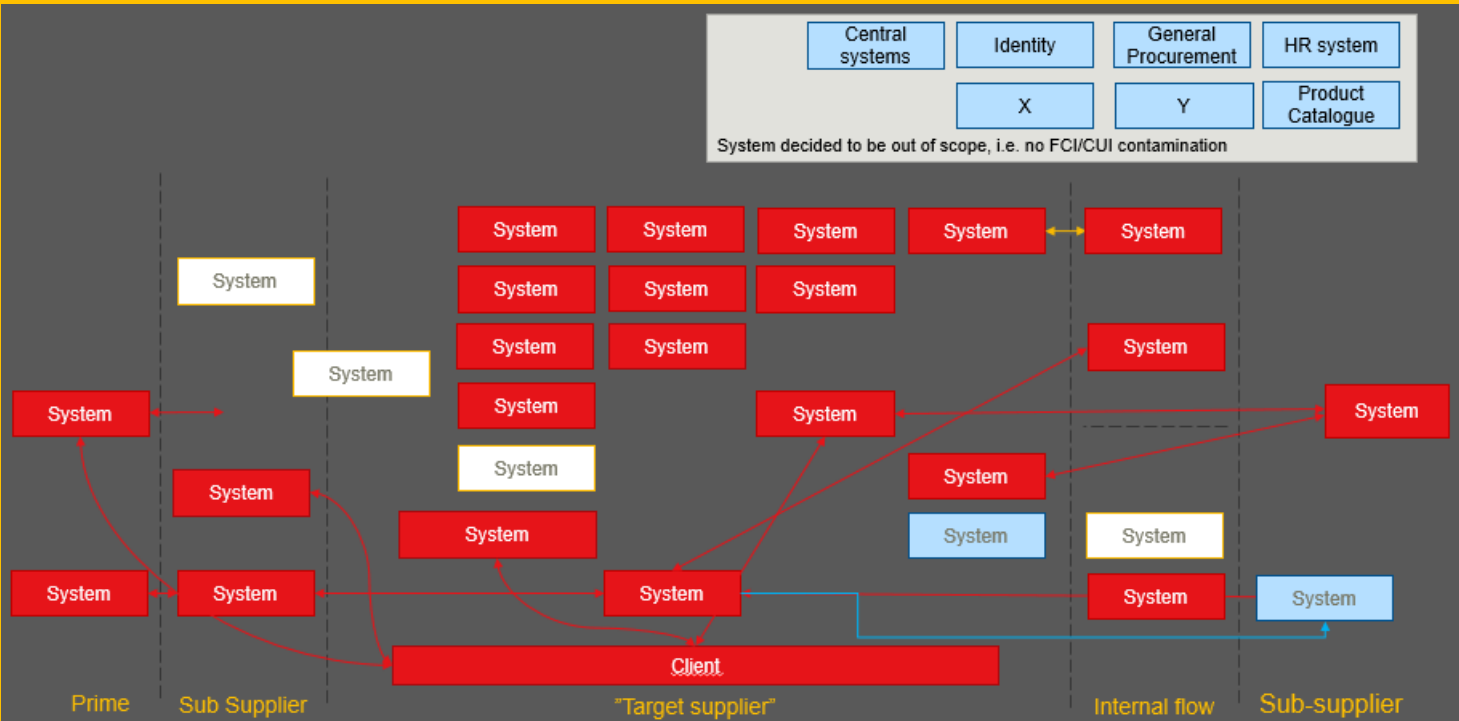
CONTRACT DATA REQUIREMENTS LIST (1 Data Item)				Form Approved OMB No. 0704-0188			
The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Department of Defense, Executive Services and Communications Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.							
Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.							
A. CONTRACT LINE ITEM NO.		B. EXHIBIT A	C. CATEGORY TDP ___ TM ___ OTHER ___ MGMT ___				
D. SYSTEM/ITEM I-MILES VTESS		E. CONTRACT/PR NO. W900RR-16-D-XXXX-XXXX		F. CONTRACTOR			
1. DATA ITEM NO. A001	2. TITLE OF THE DATA ITEM Contract Invoicing and Payment Report		3. SUBTITLE				
4. AUTHORITY (Data Requirement Document No.) DI-MGMT-81651		5. CONTRACT REFERENCE VTESS D01 SOW para 3.1.2		6. REQUIRING OFFICE			
7. DD 250 REQ LT	9. DIST STATEMENT REQUIRED F	10. FREQUENCY MONTHLY	12. DATE OF FIRST SUBMISSION See Block 16	14. DISTRIBUTION			
8. APP CODE		11. AS OF DATE NA	13. DATE OF SUBSEQUENT SUBMISSION See Block 16	a. ADDRESSEE	b. COPIES		
					Draft	Reg	Repro
16. REMARKS 1. Block 4: Contractor format is acceptable. 2. Block 9: Distribution Statement F: Further dissemination only as directed by PEO STRI or higher DOD authority; effective June 2009. Other requests for this document shall be referred to PM TRADE, 12350 Research Parkway, Orlando, FL 32826-3276.				SF AE-STRI-KOL	0	0	1
				SF AE-STRI-PMTRAD	0	0	1

17. PRICE GROUP
18. ESTIMATED TOTAL PRICE



SUPPLY CHAIN: WHATS AHEAD

METHODOLOGY



Q&A

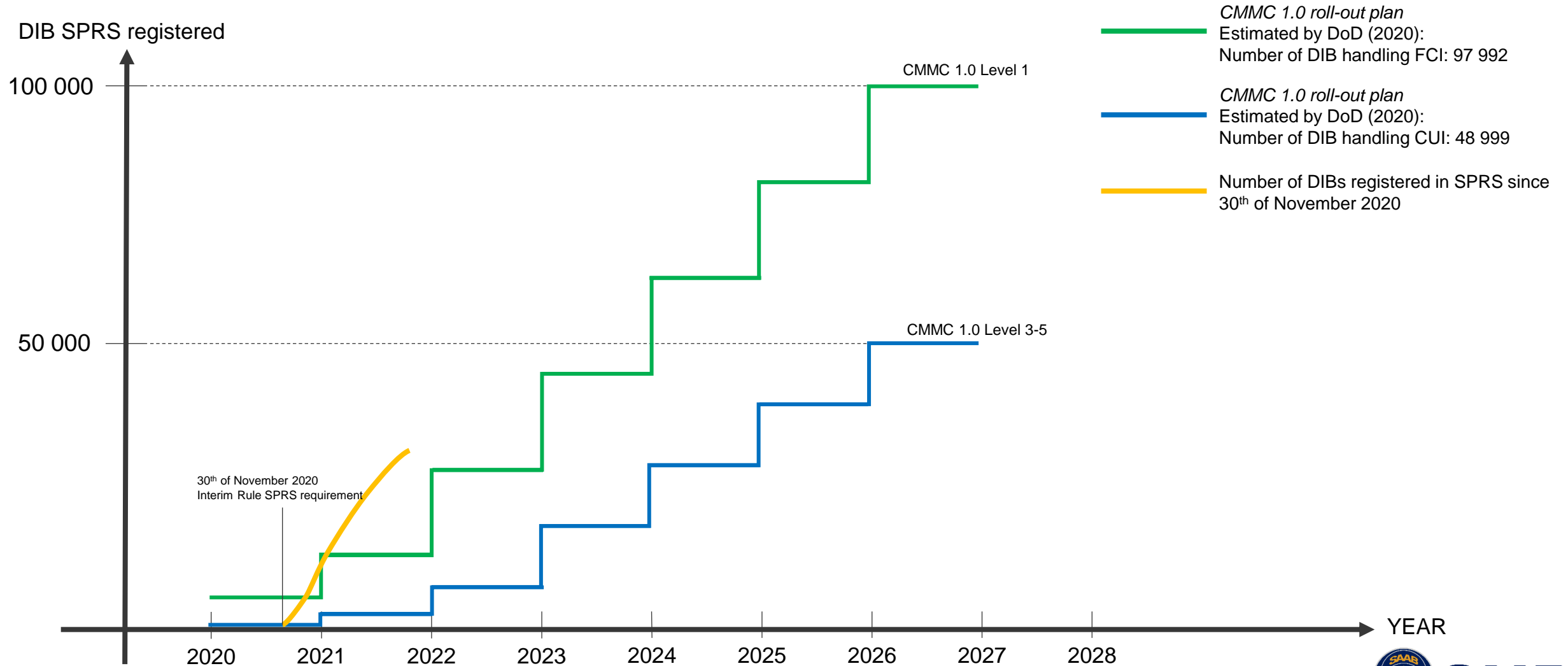


EXTRA SLIDES

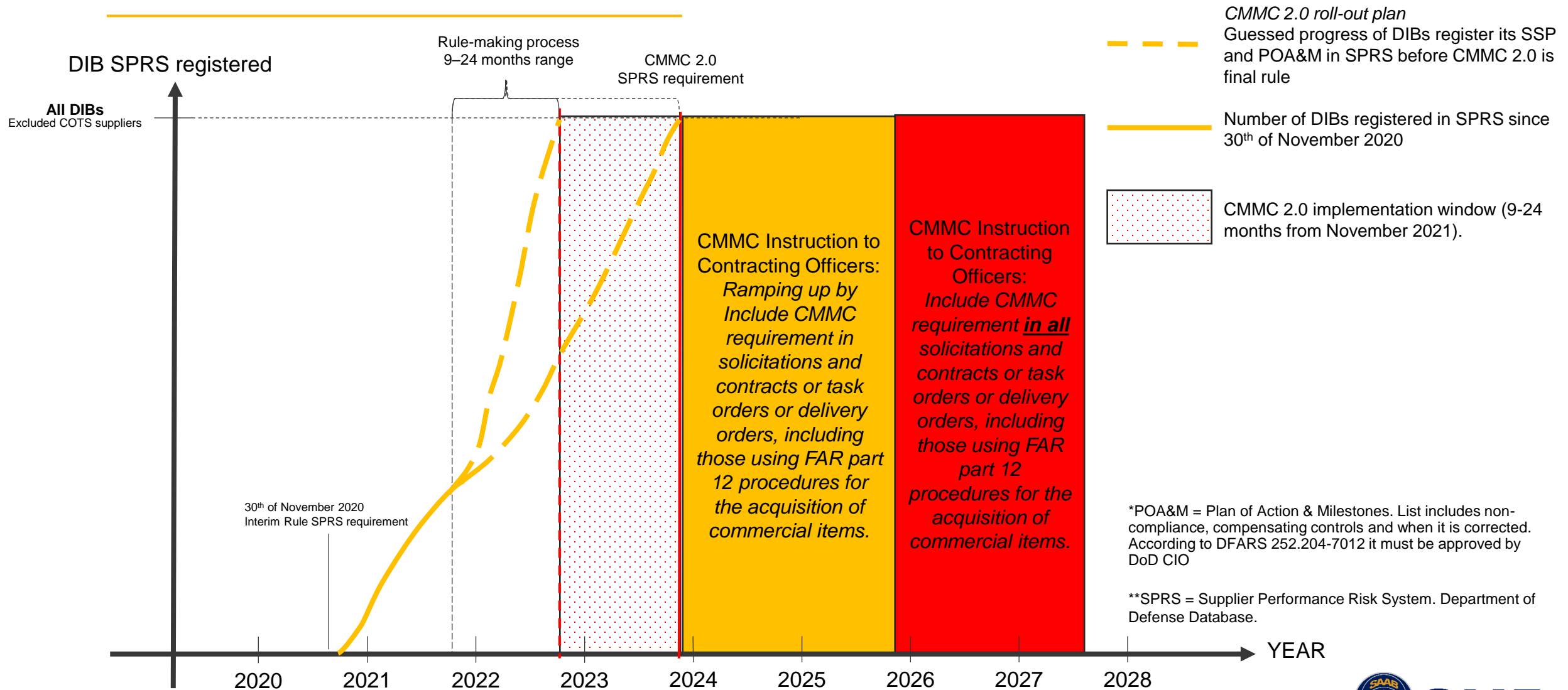
202



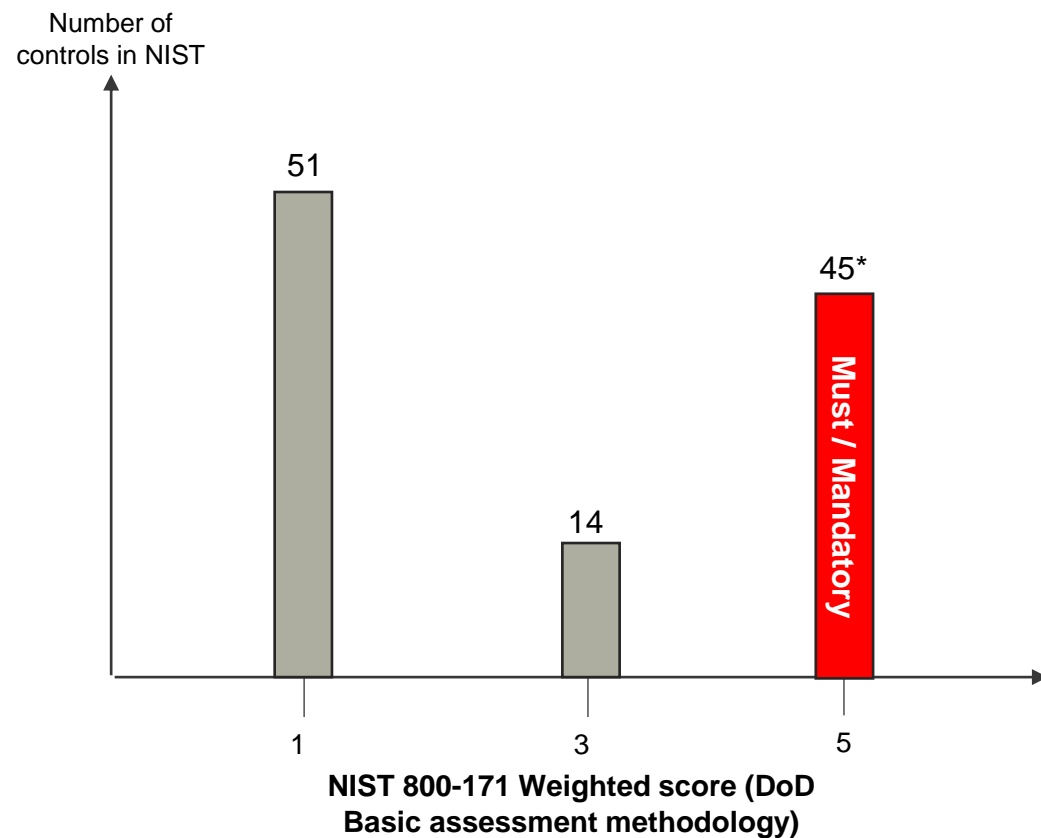
INTRODUCTION: CMMC 1.0



INTRODUCTION: CMMC 2.0



INTRODUCTION: CMMC 2.0



CMMC 2.0 have indicated that the controls can be in a POA&M but closed within **180 days**.



CMMC 2.0 have communicated that all of them must be met.

*FIPS 140-2 validated encryption will be accepted in POA&M but closed within **180 days**. This is a challenge for suppliers abroad US.

INTRODUCTION: CMMC 2.0

DFARS 252.204-7012 (2017)	CMMC 1.0 (2019)	CMMC 2.0
-	5 Certification levels	3 Certification levels: Foundational (L1 of FCI level), Advanced (L2 or CUI level) and Expert (L3 or APT level)
NIST 800-171	NIST 800-171 + 20 additional controls and process control	NIST 800-171 (anticipated to also include NFO controls)
-	3 rd party assessment and certification	Self assessment, 3 rd party assessment and DCMA DIBCAC
Self-Assessment and POA&M approved by DoD CIO	POA&M not allowed at the time for certification	POA&M allowed but not the highest-weighted requirements and need to be complete within 180 days
-	Does not allow waivers to CMMC requirement	Allow waivers to CMMC requirement under “certain limited circumstances” and will be “time-bound”
NIST 800-171 already expected to be implemented	CMMC roll-out until 2027, thereafter all contracts	Roll-out when CMMC 2.0 is finalized, i.e. expected rulemaking 9-24 months

← CMMC 2.0 Reverted back to basic, thereof the timeline should be taken seriously, i.e. within 24 months

US CYBERSECURITY WARFARE

Todays battlefield is digital!

Protection of sensitive information and critical infrastructure has with time transferred from US Government to its suppliers.

To ensure protection US Gov. implements powerful enforcement actions and certification criteria for industry.

US CYBERSECURITY WARFARE

Today's battlefield is digital!

Protection of sensitive information and critical infrastructure has with time transferred from US Government to its suppliers.

To ensure protection US Gov. implements powerful enforcement actions and certification criteria for industry.

For example:

- Foreign Ownership, Control or Influence (FOCI).
- US Gov. Acquisition framework
- Defense technology programs
- Standards and certifications
- Foreign trade with for example sensitive or emerging technologies

PROTECTION OF SENSITIVE INFORMATION NOT ALLOWED TO BE PUBLIC

2010



EO 13556
Controlled
Unclassified
Information
(Sensitive
Information)

2013



Public
Procurement
Clauses

2015



NARA
Implement
EO 13556
[32 CFR Part
2002](#)




- NARA have 124 Information categories registered as CUI, i.e. US Law, Regulation or Government policy forbid it to be publically available
- 124 Information Categories = will contaminate every phase of your business, e.g. solicitation information, agreement, time-, quality plan, ECP, etc.

US
Definition of Information
not allowed by Law to be
public Information


PROTECTION OF SENSITIVE INFORMATION NOT ALLOWED TO BE PUBLIC

2010




EO 13556
Controlled
Unclassified
Information
(Sensitive
Information)

2013



Public
Procurement
Clauses

2015



NARA
Implement
EO 13556
[32 CFR Part
2002](#)

2016



NIST SP
800-171



**US
Definition of Information
not allowed by Law to be
public Information**

**Government Defined
“Risk Position“**

- NARA have 124 Information categories registered as CUI, i.e. US Law, Regulation or Government policy forbid it to be publically available
- 124 Information Categories = will contaminate every phase of your business, e.g. solicitation information, agreement, time-, quality plan, ECP, etc.
- NIST defines the cybersecurity posture/maturity a supplier need to have, i.e. DoD risk position for exfiltration of CUI to adversaries.
- All information system needed to store, process, transit or protect CUI is scoped by NIST SP 800-171
- CMMC 2.0 Scoping Guide

PROTECTION OF SENSITIVE INFORMATION NOT ALLOWED TO BE PUBLIC

2010



EO 13556
Controlled
Unclassified
Information
(Sensitive
Information)

2013



Public
Procurement
Clauses

2015



NARA
Implement
EO 13556
[32 CFR Part
2002](#)

2016



NIST SP
800-171

2017



PRIME
Signed DFARS
252.204-7012



TIER 1
(Contractors
suppliers)



TIER 2
(Sub-
suppliers)



TIER...



**US
Definition of Information
not allowed by Law to be
public Information**

**Government Defined
"Risk Position"**

**Supply Chain Capability
to
Protect CUI**

“TRUST BUT VERIFY”

TRUST IS GOOD, VERIFY IS BETTER

- US Government conclusion 2018 was that TRUST based approach have not worked
- US Government Initiated Cybersecurity Maturity Model Certification (CMMC) Initiative 2019 as a VERIFY based approach by third party assessor.



“TRUST BUT VERIFY”

TRUST IS GOOD, VERIFY IS BETTER

- US Government conclusion 2018 was that TRUST based approach have not worked
- US Government Initiated Cybersecurity Maturity Model Certification (CMMC) Initiative 2019 as a VERIFY based approach by third party assessor.

CARROT AND STICK

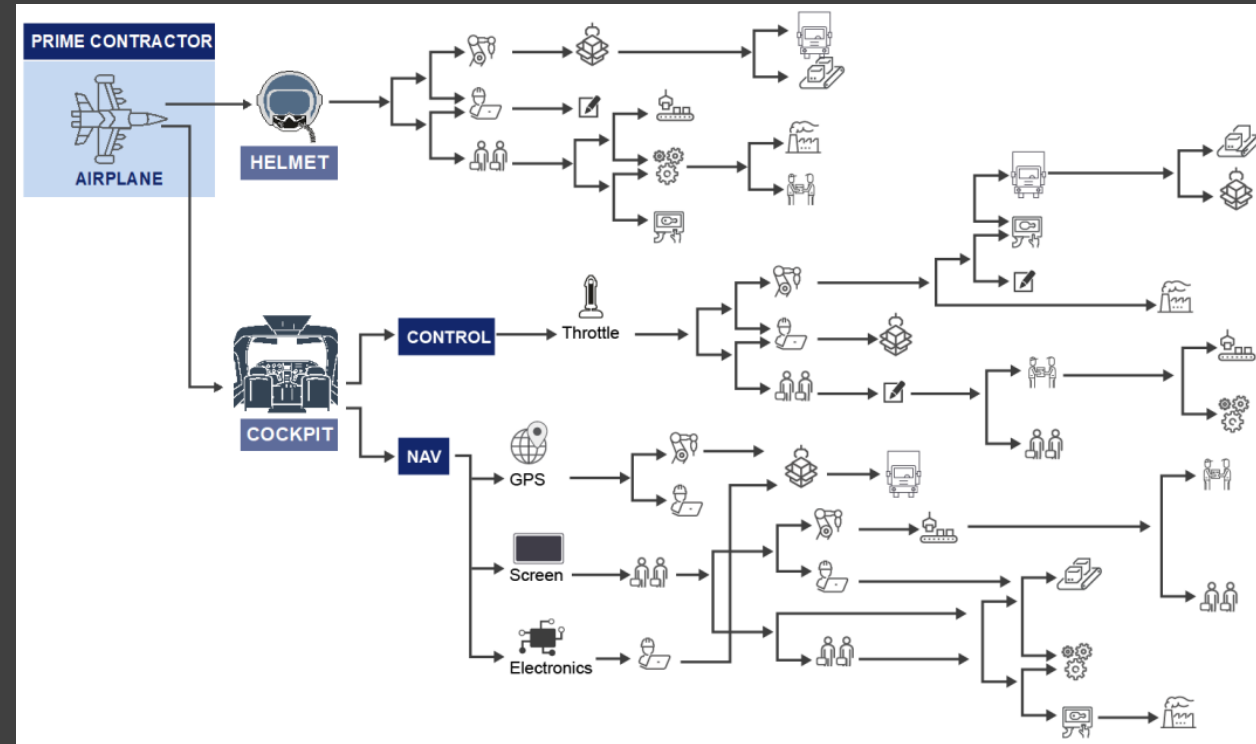
- Carrot
 - The contractor or sub-supplier remains in the supply chain
- Stick
 - Financial consequences (fines, withholding payment etc.)
 - Cancellation of contract,
 - Termination as supplier (blacklisting) to US Government
 - False cybersecurity compliance statements from suppliers may result in criminal liability (False Claims Act).
 - Department of Justice (DoJ) stated that false cybersecurity compliance statements is on the priority list. Source: [Department of Justice](#)



SUPPLY CHAIN IMPACT WITH “VERIFY”

HOW DOES CUSTOMER “VERIFY” APPROACH AFFECT CONTRACTORS SUPPLY CHAIN?

- US Government makes the contractor Ultimately responsible for its Supply Chain
- Enforcing a “Verify” approach requiring not only that Contractor is Certified, but also its Supply Chain that need to handle Sensitive Information.



Source: [DAU](#) (2020)

SUPPLY CHAIN: WHATS AHEAD

THE PATH FORWARD WILL BE LIMITED

1. In-house, take back production

“Cyber insurers have become more aware of ambiguities in their insurance in recent years, but some are slower to adapt than others.”

“Any time there's ambiguous wording on a policy, it's to the client's advantage, not the insurer's.”

Source: [Reuters](#) (31 March 2022)

SUPPLY CHAIN: WHATS AHEAD

THE PATH FORWARD WILL BE LIMITED

1. In-house, take back production
2. Choose Strategical Suppliers with the same challenge and interest to solve it with you

“Cyber insurers have become more aware of ambiguities in their insurance in recent years, but some are slower to adapt than others.”

“Any time there's ambiguous wording on a policy, it's to the client's advantage, not the insurer's.”

Source: [Reuters](#) (31 March 2022)

SUPPLY CHAIN: WHATS AHEAD

THE PATH FORWARD WILL BE LIMITED

1. In-house, take back production
2. Choose Strategical Suppliers with the same challenge and interest to solve it with you
3. Provide suppliers with IT solution, i.e. build you own collaboration/supplier cloud

“Cyber insurers have become more aware of ambiguities in their insurance in recent years, but some are slower to adapt than others.”

“Any time there's ambiguous wording on a policy, it's to the client's advantage, not the insurer's.”

Source: [Reuters](#) (31 March 2022)

SUPPLY CHAIN: WHATS AHEAD

THE PATH FORWARD WILL BE LIMITED

1. In-house, take back production
2. Choose Strategical Suppliers with the same challenge and interest to solve it with you
3. Provide suppliers with IT solution, i.e. build you own collaboration/supplier cloud
4. Address to the Government of the need of a nation cloud

“Cyber insurers have become more aware of ambiguities in their insurance in recent years, but some are slower to adapt than others.”

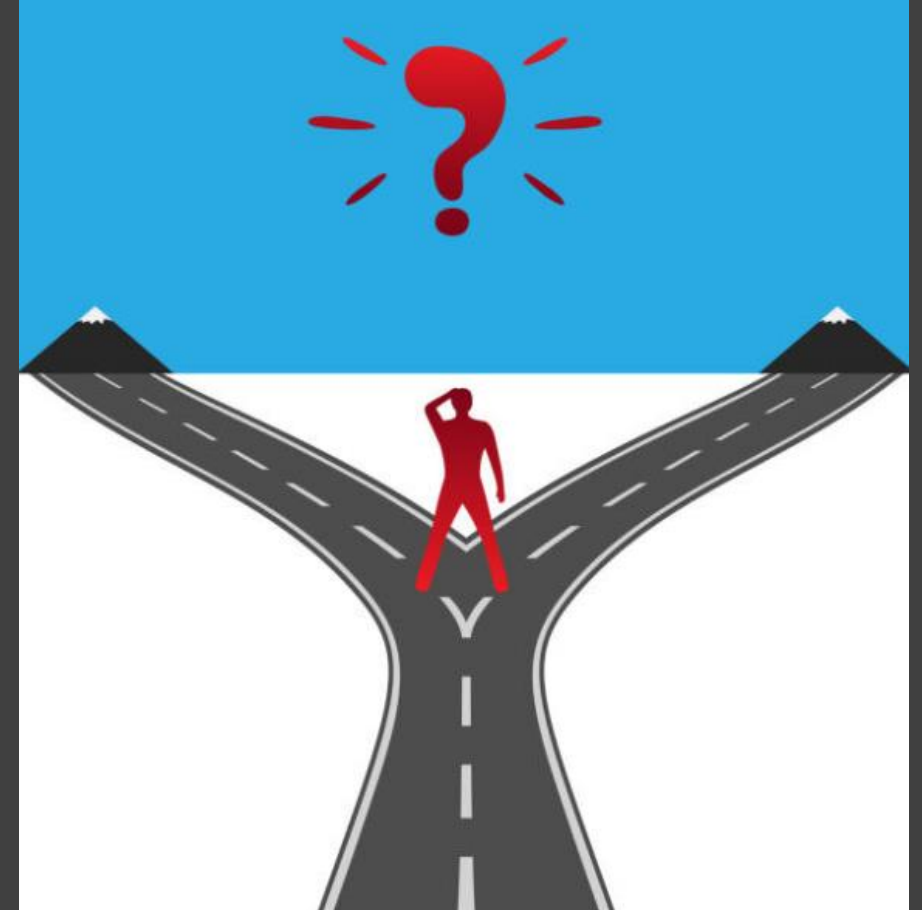
“Any time there's ambiguous wording on a policy, it's to the client's advantage, not the insurer's.”

Source: [Reuters](#) (31 March 2022)

SUPPLY CHAIN: WHATS AHEAD

IF YOU ARE A SMALL, MEDIUM BUSINESS

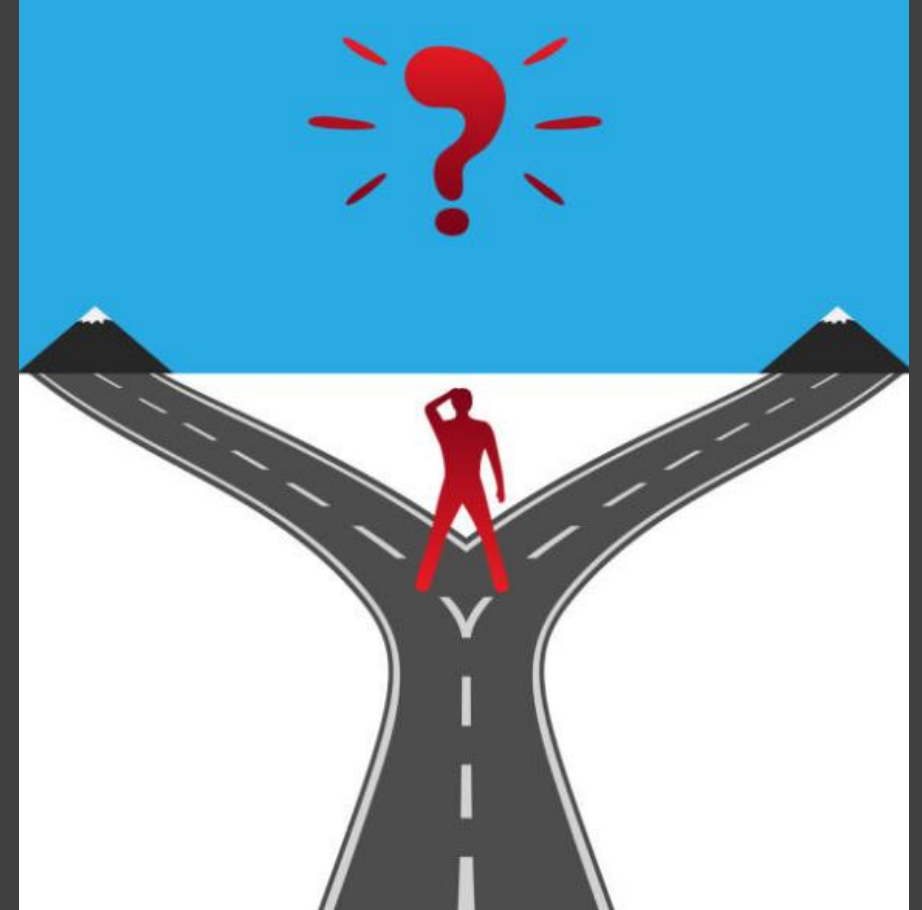
1. Think of which contracts and customer you want!



SUPPLY CHAIN: WHATS AHEAD

IF YOU ARE A SMALL, MEDIUM BUSINESS

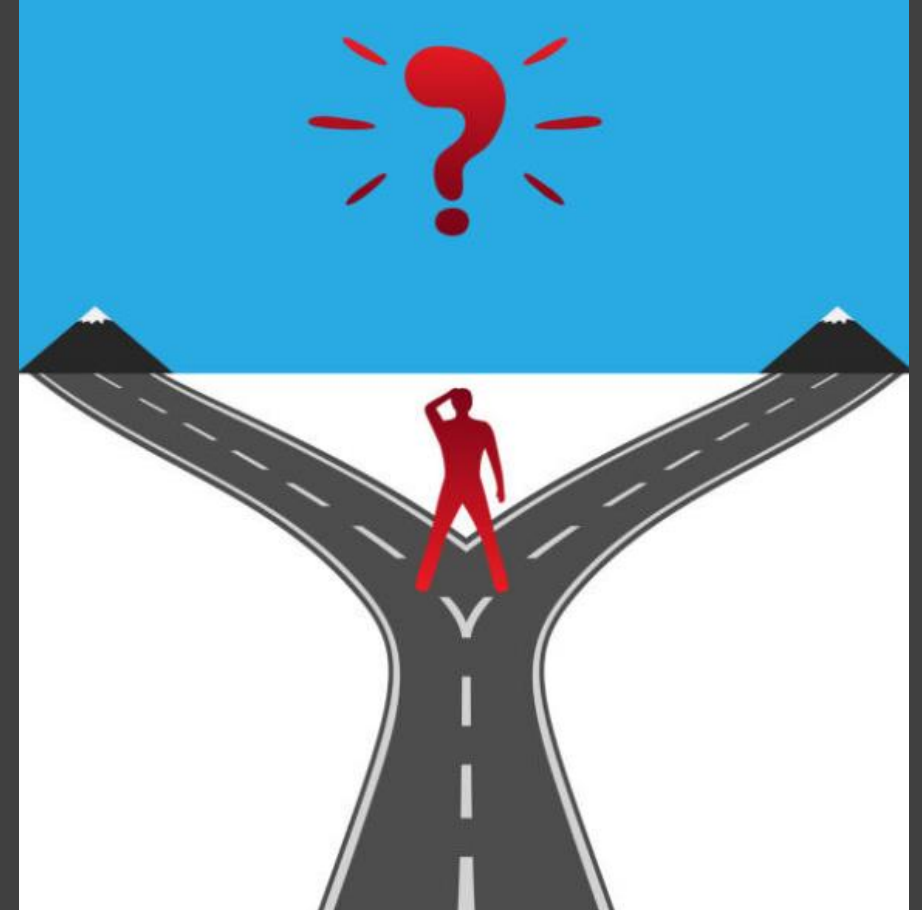
1. Think of which contracts and customer you want!
2. Ask yourself: What is our cybersecurity baseline today, do we have a supportive Architecture?



SUPPLY CHAIN: WHATS AHEAD

IF YOU ARE A SMALL, MEDIUM BUSINESS

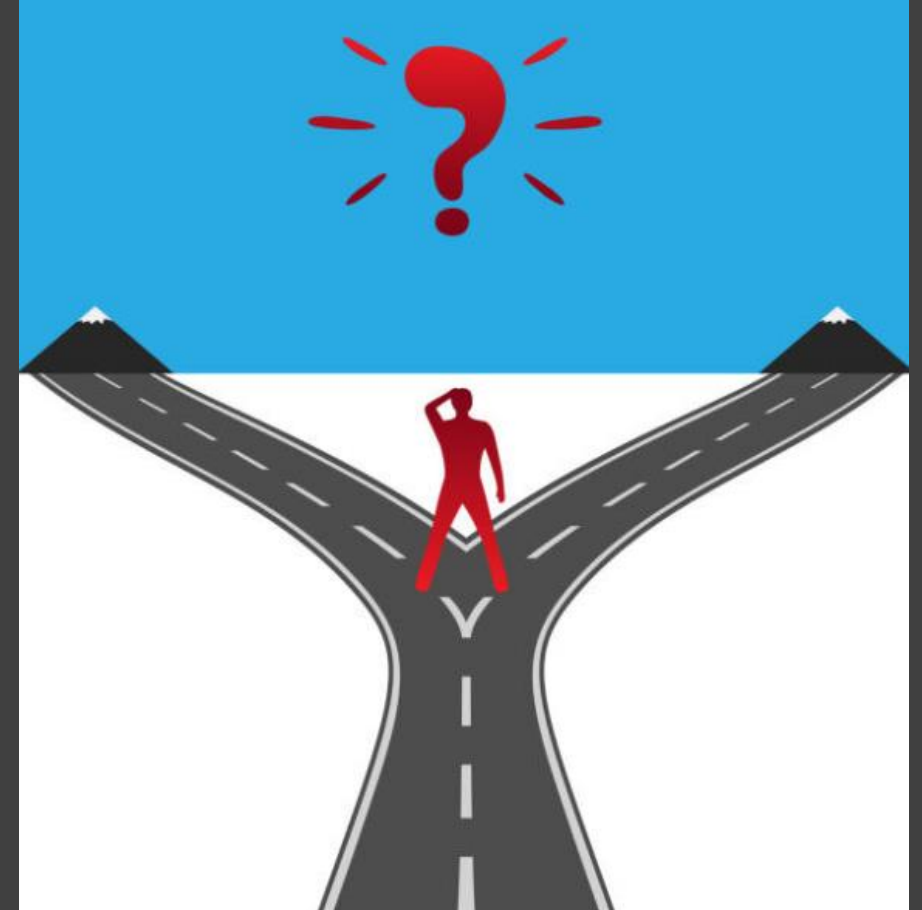
1. Think of which contracts and customer you want!
2. Ask yourself: What is our cybersecurity baseline today, do we have a supportive Architecture?
3. Ask if the customer can provide a collaboration service. With that the responsibility to protect the sensitive information remains with the customer.



SUPPLY CHAIN: WHATS AHEAD

IF YOU ARE A SMALL, MEDIUM BUSINESS

1. Think of which contracts and customer you want!
2. Ask yourself: What is our cybersecurity baseline today, do we have a supportive Architecture?
3. Ask if the customer can provide a collaboration service. With that the responsibility to protect the sensitive information remains with the customer.
4. **Have a long term goal, you may need to say No to contracts along the way!**



SUPPLY CHAIN: WHATS AHEAD

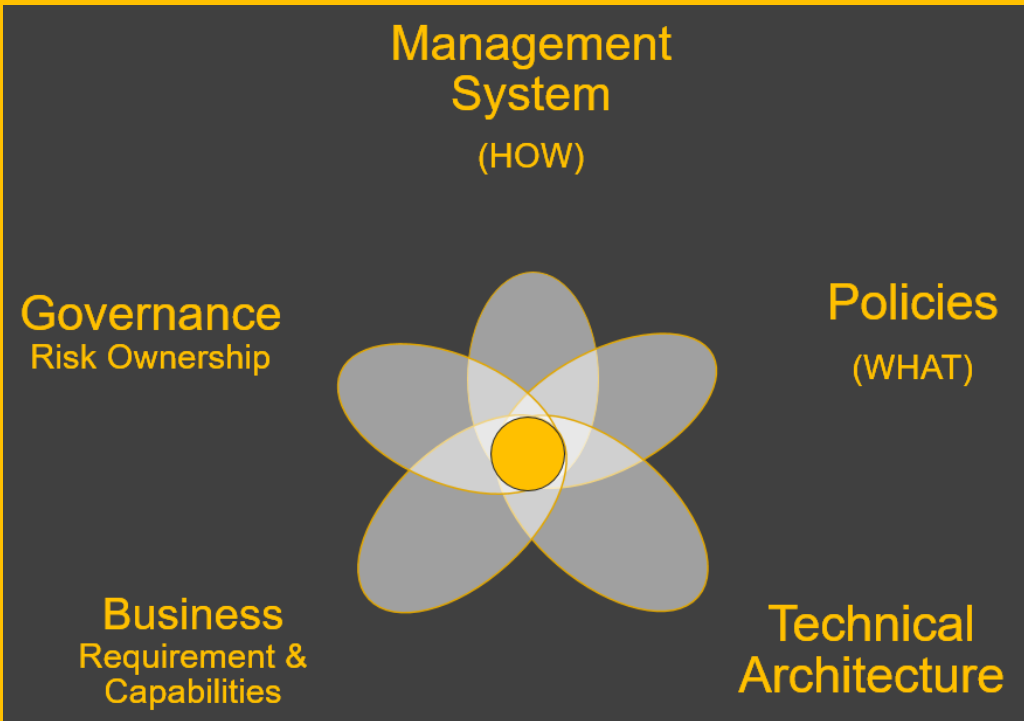
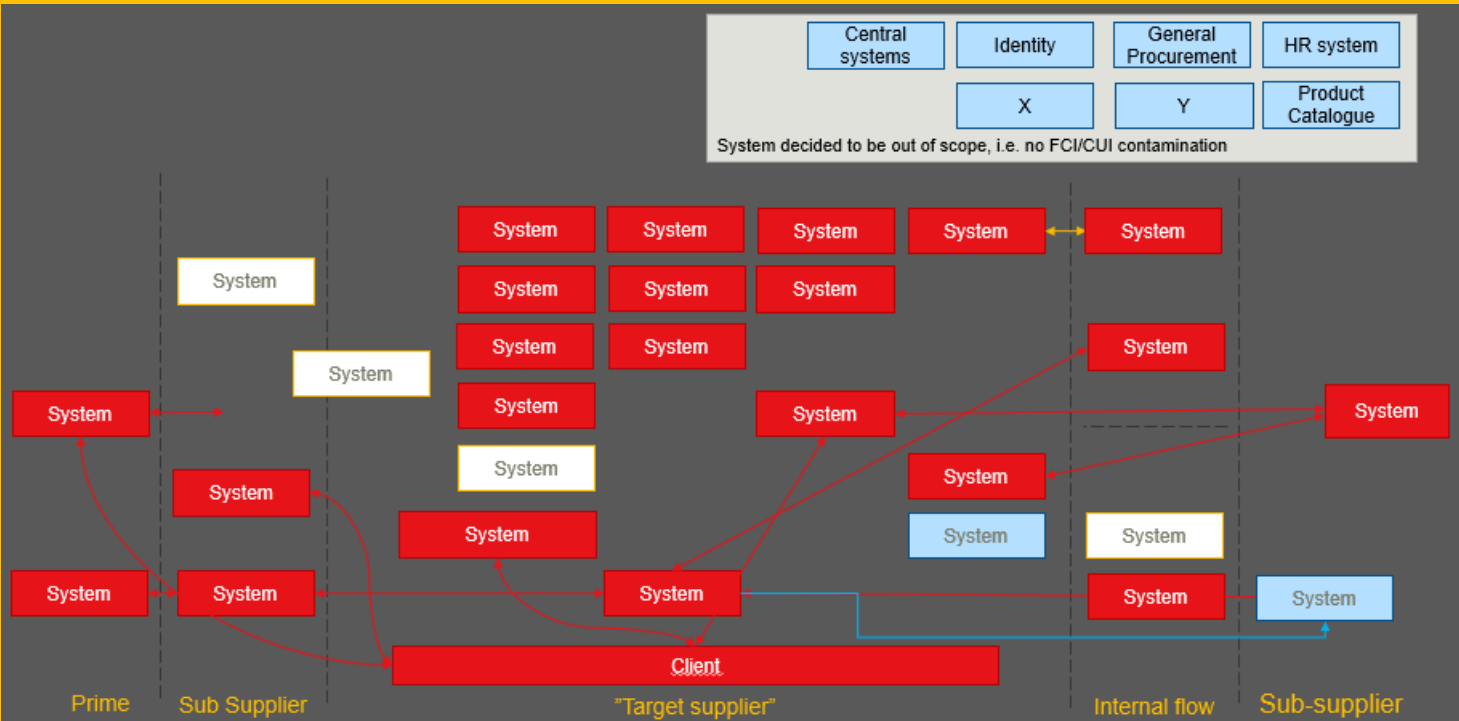
IF YOU ARE A LARGE ENTERPRISE

- Ask yourself: What is our cybersecurity baseline today, do we have a supportive Enterprise Architecture?



SUPPLY CHAIN: WHATS AHEAD

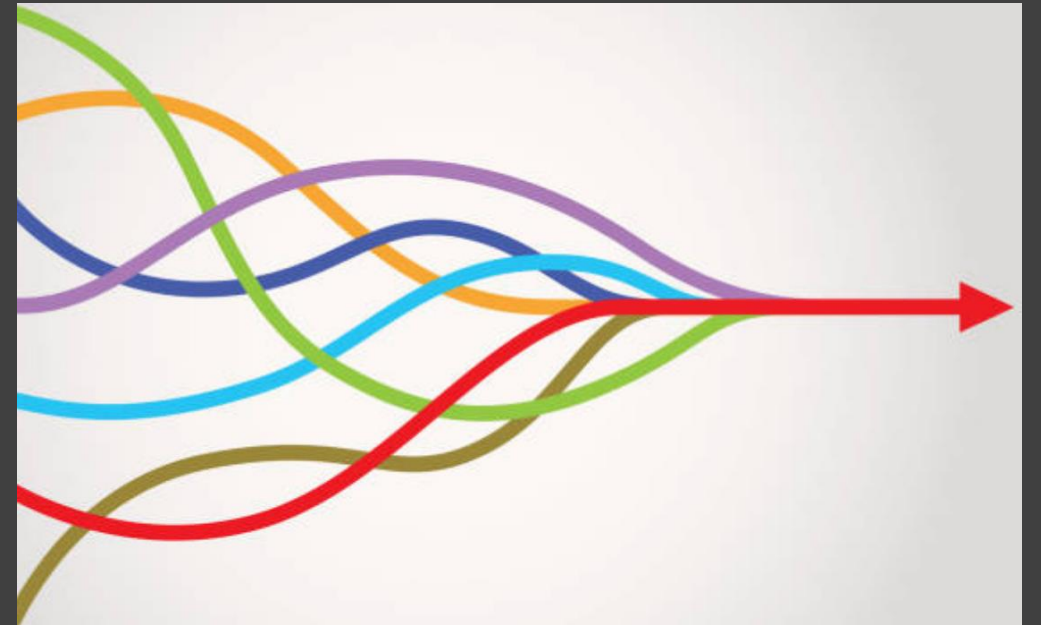
METHODOLOGY



SUPPLY CHAIN: WHATS AHEAD

IF YOU ARE A LARGE ENTERPRISE

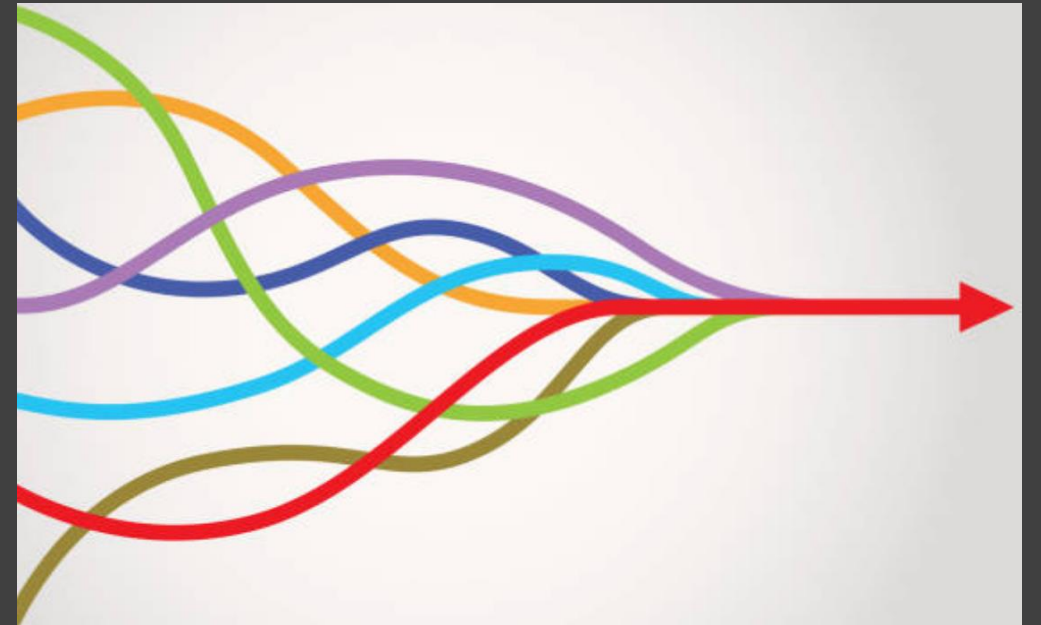
- Ask yourself: What is our cybersecurity baseline today, do we have a supportive Enterprise Architecture?
- Are we dependent on Cloud-provider?



SUPPLY CHAIN: WHATS AHEAD

IF YOU ARE A LARGE ENTERPRISE

- Ask yourself: What is our cybersecurity baseline today, do we have a supportive Enterprise Architecture?
- Are we dependent on Cloud-provider?
- Do I know what type of cloud services is compliant to be used?
 - “Compliance” Vs “Cybersecurity” aspect



SUPPLY CHAIN: WHATS AHEAD

IF YOU ARE A LARGE ENTERPRISE

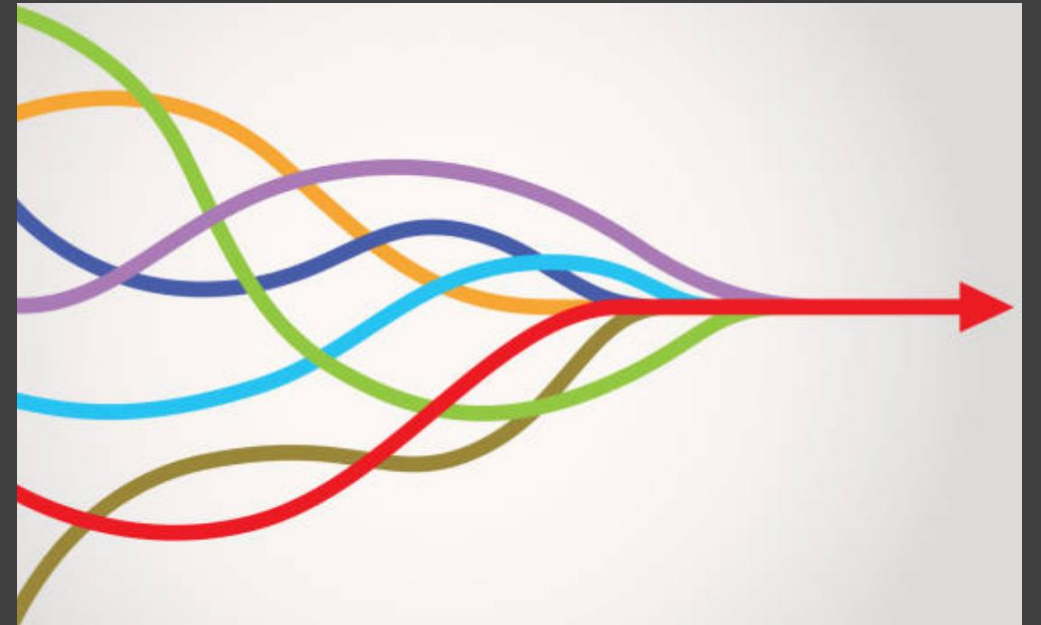
- Ask yourself: What is our cybersecurity baseline today, do we have a supportive Enterprise Architecture?
- Are we dependent on Cloud-provider?
- Do I know what type of cloud services is compliant to be used?
 - “Compliance” Vs “Cybersecurity” aspect
- Ask yourself: Do I know our supply-chain cybersecurity baseline and how many Tiers we have?



SUPPLY CHAIN: WHATS AHEAD

IF YOU ARE A LARGE ENTERPRISE

- Ask yourself: What is our cybersecurity baseline today, do we have a supportive Enterprise Architecture?
- Are we dependent on Cloud-provider?
- Do I know what type of cloud services is compliant to be used?
 - Compliance Vs Cybersecurity aspect
- Ask yourself: Do I know our supply-chain cybersecurity baseline and how many Tiers we have?
- **Is it necessary to flow down Sensitive Information to our Supply Chain?**



SUMMARY OF THE MEGATREND





Thank you

Urban Lyxzén Bervelius
