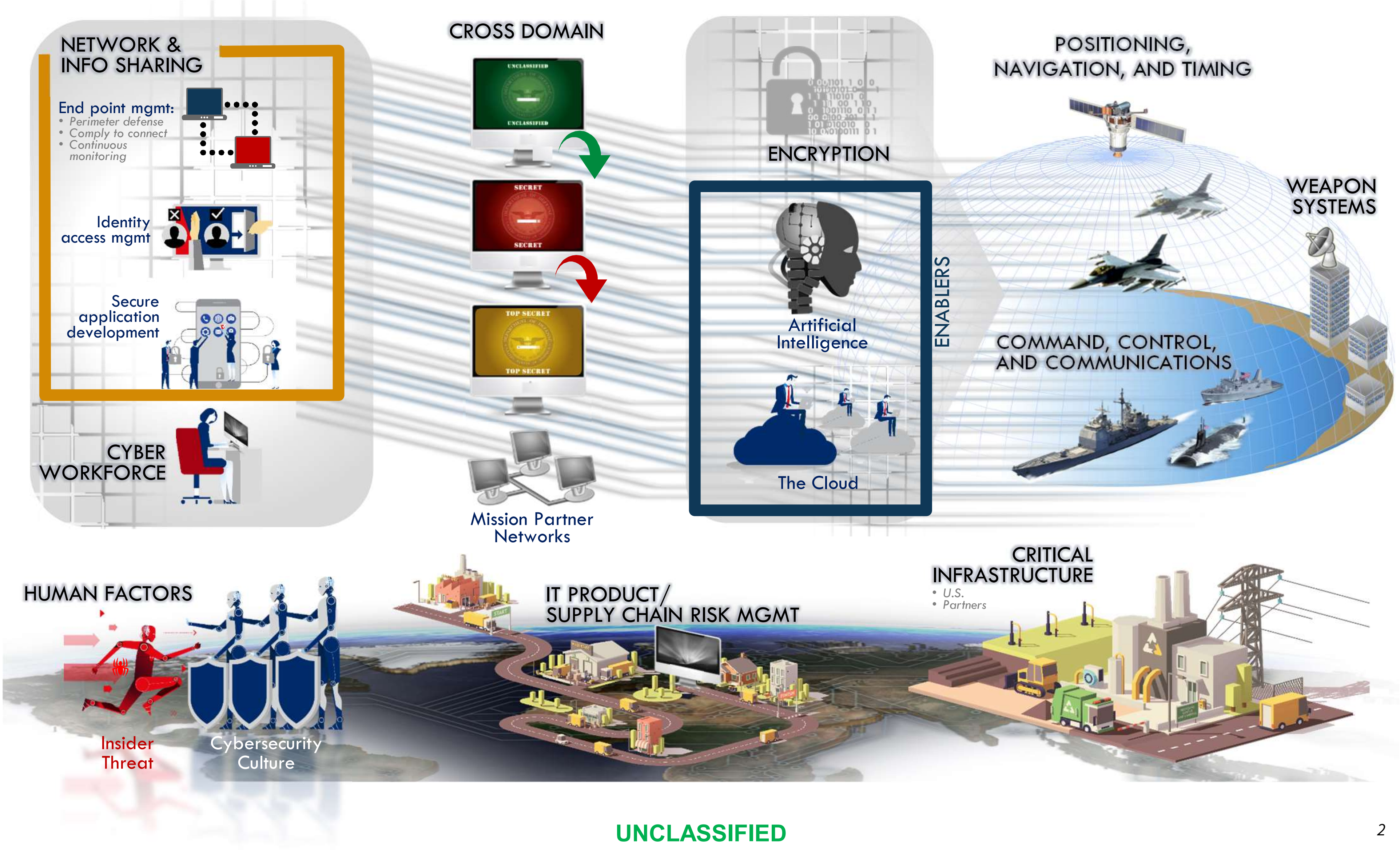
Securing the Supply Chain

What is the DoD Supply Chain



NETWORK & INFO SHARING

End point mgmt:
- Perimeter defense
- Comply to connect
- Continuous monitoring

Identity access mgmt

Secure application development

CYBER WORKFORCE

CROSS DOMAIN

Mission Partner Networks

ENCRYPTION

ENABLERS

Artificial Intelligence

The Cloud

POSITIONING, NAVIGATION, AND TIMING

WEAPON SYSTEMS

COMMAND, CONTROL, AND COMMUNICATIONS

HUMAN FACTORS

Insider Threat

Cybersecurity Culture

IT PRODUCT/ SUPPLY CHAIN RISK MGMT

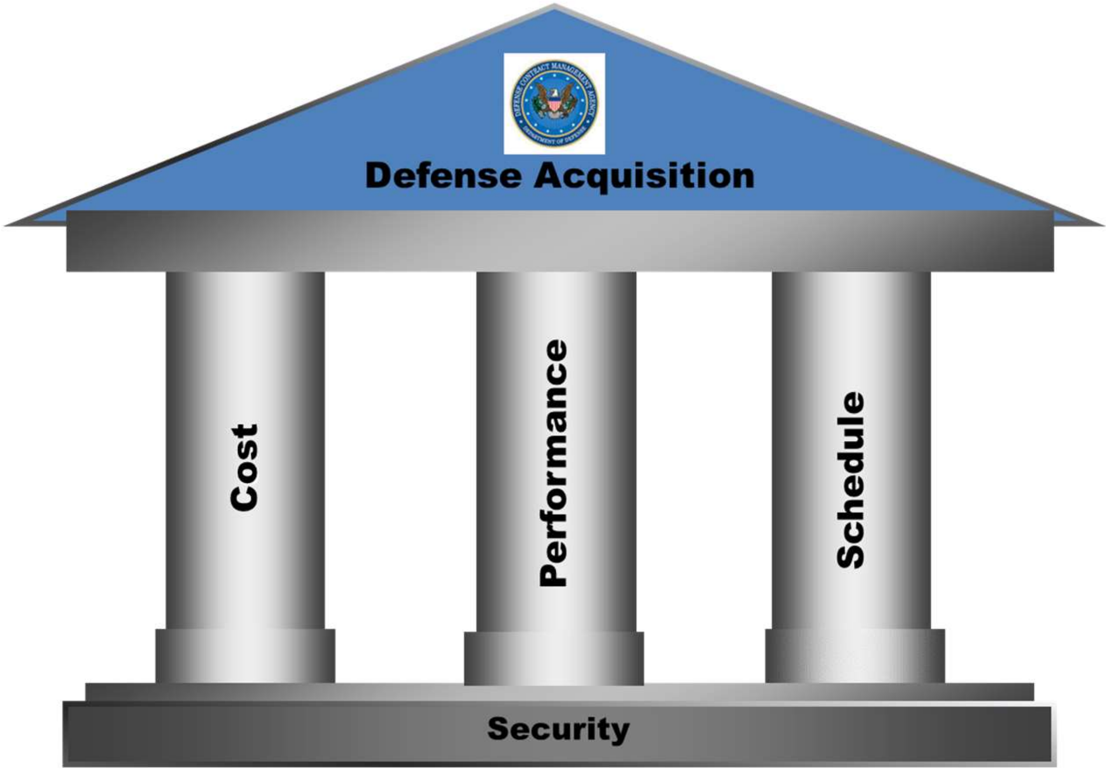
CRITICAL INFRASTRUCTURE
- U.S.
- Partners

UNCLASSIFIED

We need to make Security the Foundation
We need to Deliver Uncompromised

Cost, Schedule, Performance

ARE ONLY EFFECTIVE IN A SECURE ENVIROMENT



UNCLASSIFIED

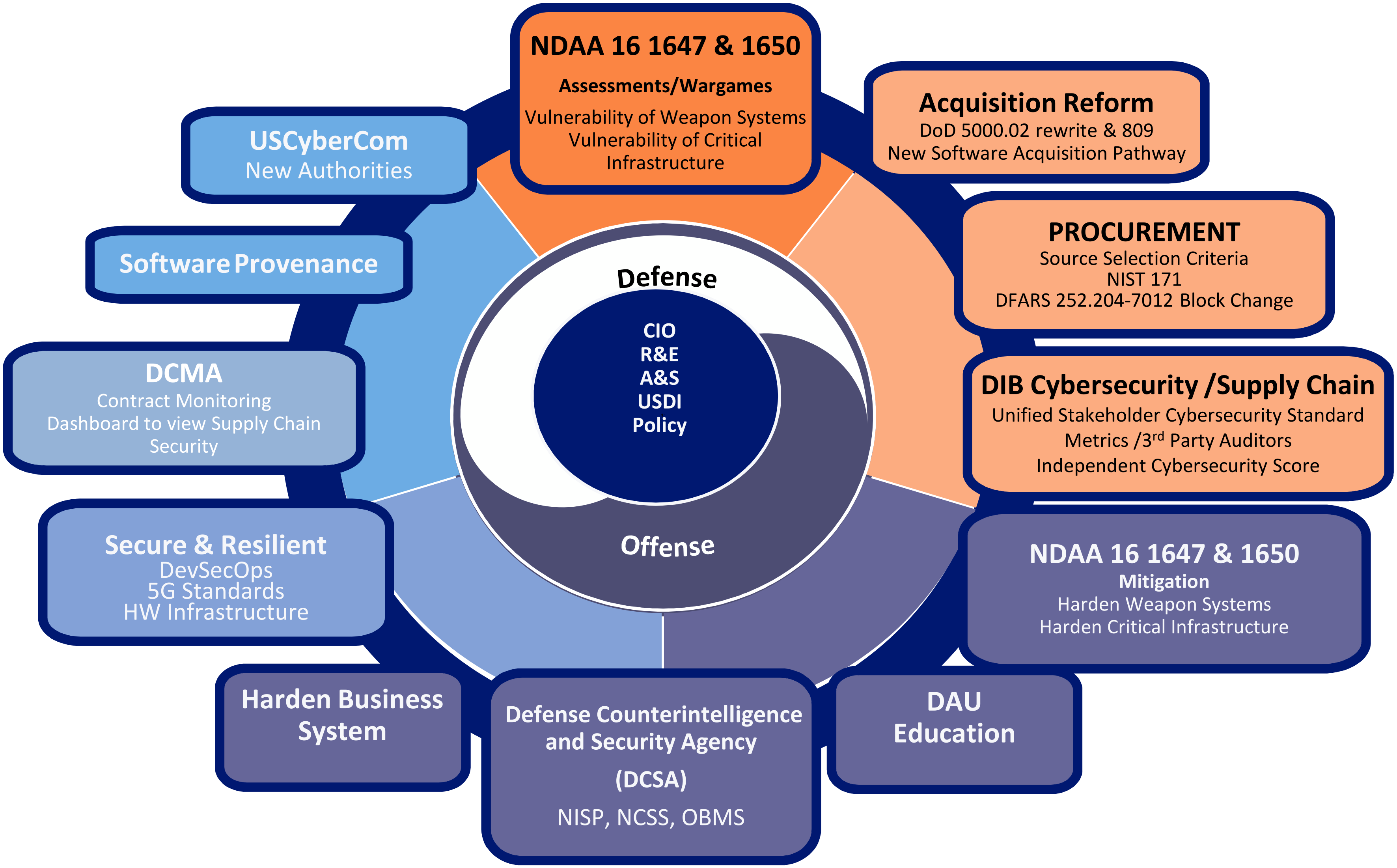
Delivered Uncompromised by Mitre

5 Key Structural Challenges

15 Recommended Courses of Action

“We need risk management solutions to assess, measure, and mitigate risk in real-time across multi-tier partner and supplier networks to achieve our goal of cost, schedule and performance, as they are only effective in a secure environment.” The Honorable Kevin Fahey, Assistant Secretary of Defense for Acquisition

Securing the DoD Acquisition Ecosystem



NDAA 16 1647 & 1650
Assessments/Wargames
Vulnerability of Weapon Systems
Vulnerability of Critical Infrastructure

Acquisition Reform
DoD 5000.02 rewrite & 809
New Software Acquisition Pathway

PROCUREMENT
Source Selection Criteria
NIST 171
DFARS 252.204-7012 Block Change

DIB Cybersecurity /Supply Chain
Unified Stakeholder Cybersecurity Standard
Metrics /3rd Party Auditors
Independent Cybersecurity Score

NDAA 16 1647 & 1650
Mitigation
Harden Weapon Systems
Harden Critical Infrastructure

DAU
Education

Defense Counterintelligence and Security Agency
(DCSA)
NISP, NCSS, OBMS

Harden Business System

Secure & Resilient
DevSecOps
5G Standards
HW Infrastructure

DCMA
Contract Monitoring
Dashboard to view Supply Chain Security

Software Provenance

USCyberCom
New Authorities

Defense

CIO
R&E
A&S
USDI
Policy

Offense

Cybersecurity Maturity Model Certification (CMMC)

- The DoD is working with John Hopkins University Applied Physics Laboratory (APL) and Carnegie Mellon University Software Engineering Institute (SEI) to review and combine various cybersecurity standards into one unified standard for cybersecurity.

- The new standard and maturity model will be named Cybersecurity Maturity Model Certification (CMMC)

- The CMMC levels will range from basic hygiene to “State-of-the-Art” and will also capture both security control and the institutionalization of processes that enhance cybersecurity for DIB companies.

- The required CMMC level (notionally between 1 – 5) for a specific contract will be contained in the RFP sections L & M, and will be a “go/no-go decision”.

- The CMMC must be semi-automated and, more importantly, cost effective enough so that Small Businesses can achieve the minimum CMMC level of 1.

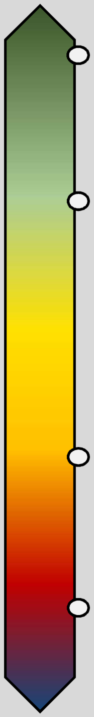
- The CMMC model will be agile enough to adapt to emerging and evolving cyber threats to the DIB sector. A neutral 3rd party will maintain the standard for the Department.

- The CMMC will include a center for cybersecurity education and training.

- The CMMC will include the development and deployment of a tool that 3rd party cybersecurity certifiers will use to conduct audits, collect metrics, and inform risk mitigation for the entire supply chain.

DIB Cybersecurity Posture

Hypothesis:
< 1% of DIB companies



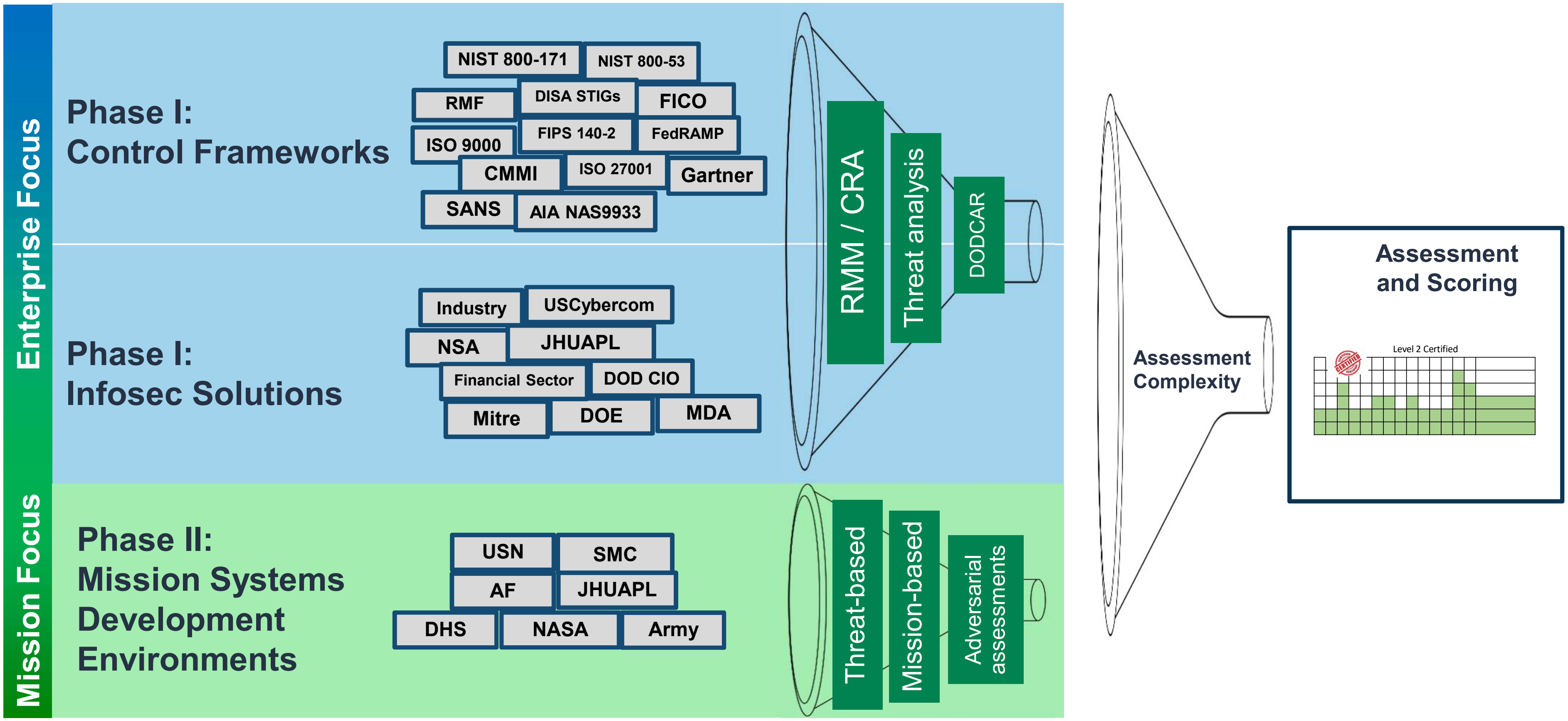
- **State-of-the-Art**
  - Maneuver, Automation, SecDevOps
- **Nation-state**
  - Resourcing: Infosec dedicated full-time staff ≥ 4, Infosec ≥ 10% IT budget
  - Sophisticated TTPs: Hunt, white listing, limited Internet access, air-gapped segments
  - Culture: Operations-impacting InfoSec authority, staff training and test

---

- **Good cyber hygiene**
  - NIST SP 800-171 compliant, etc.
  - Consistently defends against Tier I-II attacks
- **Ad hoc**
  - Inconsistent cyber hygiene practices
  - Low-level attacks succeed consistently

Vast majority of DIB companies →

Notional CMMC Model Development



Enterprise Focus

Phase I:
Control Frameworks

NIST 800-171
NIST 800-53
RMF
DISA STIGs
FICO
ISO 9000
FIPS 140-2
FedRAMP
CMMI
ISO 27001
Gartner
SANS
AIA NAS9933

Phase I:
Infosec Solutions

Industry
USCybercom
NSA
JHUAPL
Financial Sector
DOD CIO
Mitre
DOE
MDA

RMM / CRA
Threat analysis
DODCAR

Mission Focus

Phase II:
Mission Systems
Development
Environments

USN
SMC
AF
JHUAPL
DHS
NASA
Army

Threat-based
Mission-based
Adversarial assessments

Assessment Complexity

Assessment and Scoring

Maturity model must be dynamic and threat informed

Notional CMMC Model Components

Sophistication of Practices -- AND -- Institutionalization of Processes

Notional CMMC Level	Access Control (22*)	Awareness & Training (3*)	Audit & Accountability (9*)	●●●	Security Assessment (4*)	Systems & Comms. Protection (16*)	System & Info Integrity (7*)
5						△	
4	△		△			△	
3	△△△		△△	●●●		△	
2	△△△△△△	△	△△△			△△△	△△△
1	△△△△△△△△△△△△	△△	△△△		△△△△	△△△△△△△△△△	△△△△

All 14 Control Families

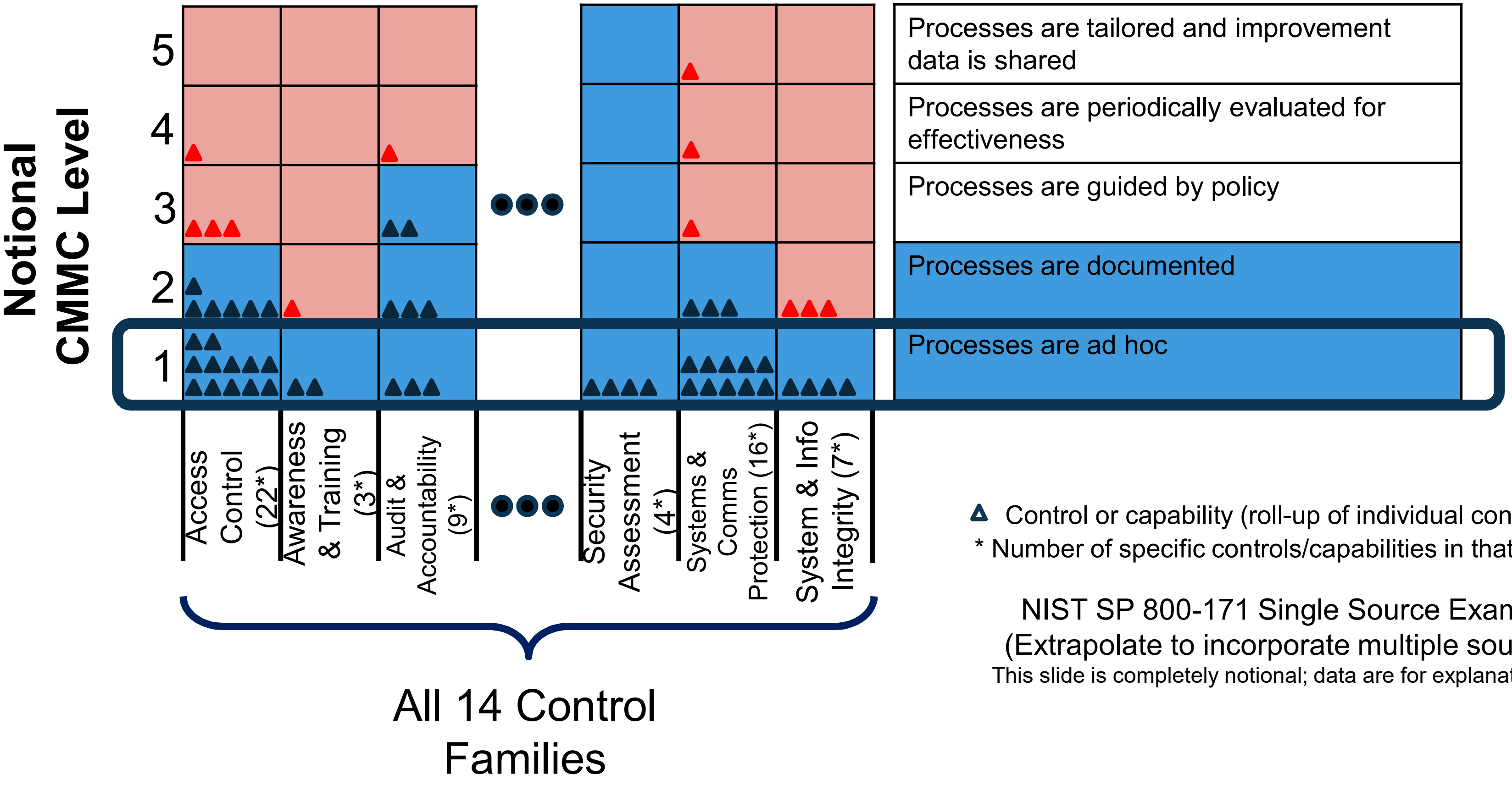
Processes are tailored and improvement data is shared	5
Practices are periodically evaluated for effectiveness	4
Processes are guided by policy	3
Processes are documented	2
Processes are ad hoc	1

△ Control or capability (roll-up of individual controls)

* Number of specific controls/capabilities in that control family

NIST SP 800-171 Single Source Example
(Extrapolate to incorporate multiple sources)
This slide is completely notional; data are for explanation only

Notional CMMC Level 1



Notional CMMC Level

5 Processes are tailored and improvement data is shared

4 Processes are periodically evaluated for effectiveness

3 Processes are guided by policy

2 Processes are documented

1 Processes are ad hoc

Access Control (22*)

Awareness & Training (3*)

Audit & Accountability (9*)

●●●

Security Assessment (4*)

Systems & Comms Protection (16*)

System & Info Integrity (7*)

All 14 Control Families

▲ Control or capability (roll-up of individual controls)

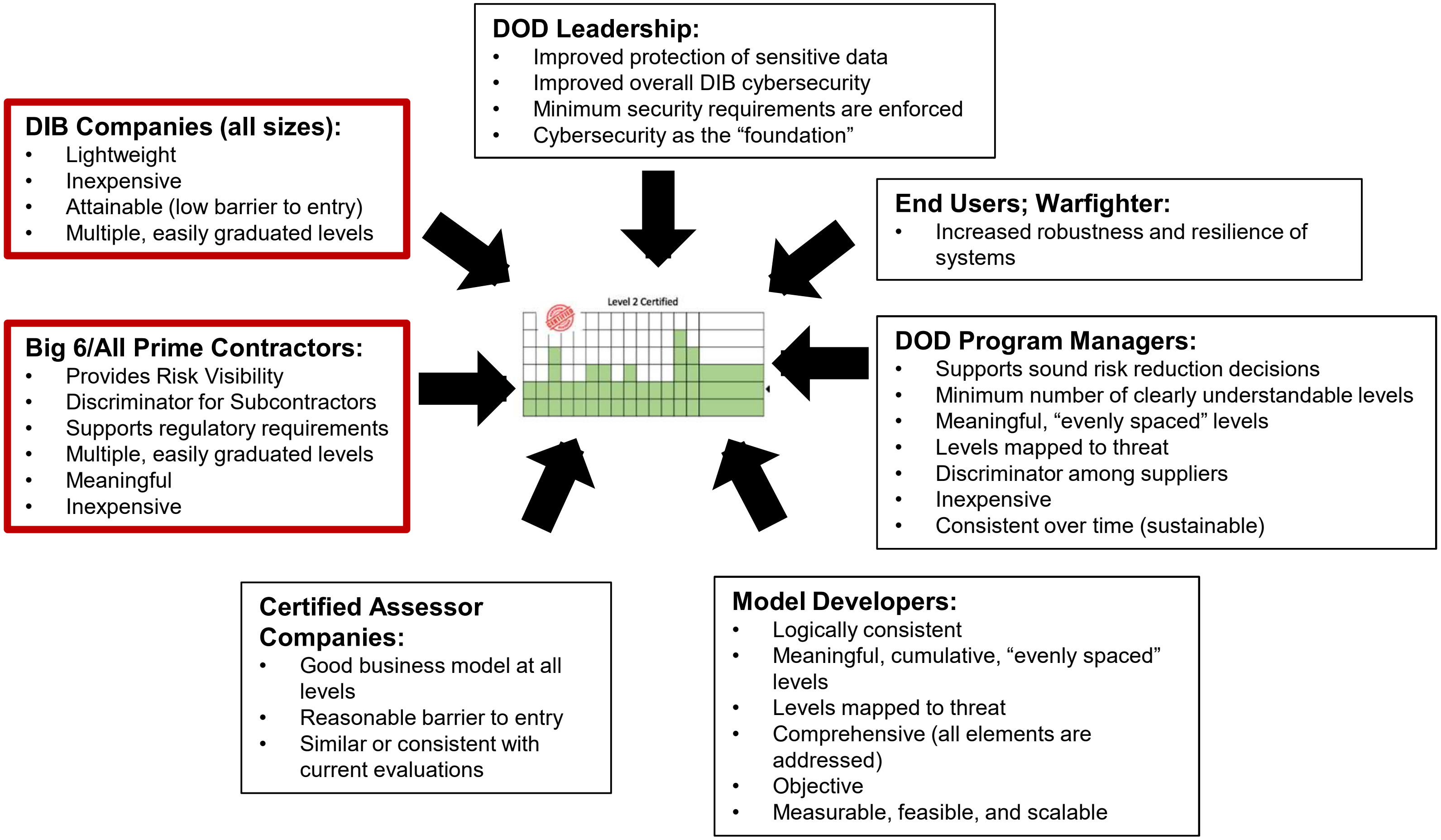
* Number of specific controls/capabilities in that control family

NIST SP 800-171 Single Source Example
(Extrapolate to incorporate multiple sources)

This slide is completely notional; data are for explanation only

UNCLASSIFIED

Preliminary Stakeholder Perspectives on CMMC



DOD Leadership:

- Improved protection of sensitive data
- Improved overall DIB cybersecurity
- Minimum security requirements are enforced
- Cybersecurity as the "foundation"

DIB Companies (all sizes):

- Lightweight
- Inexpensive
- Attainable (low barrier to entry)
- Multiple, easily graduated levels

End Users; Warfighter:

- Increased robustness and resilience of systems

Big 6/All Prime Contractors:

- Provides Risk Visibility
- Discriminator for Subcontractors
- Supports regulatory requirements
- Multiple, easily graduated levels
- Meaningful
- Inexpensive

DOD Program Managers:

- Supports sound risk reduction decisions
- Minimum number of clearly understandable levels
- Meaningful, "evenly spaced" levels
- Levels mapped to threat
- Discriminator among suppliers
- Inexpensive
- Consistent over time (sustainable)

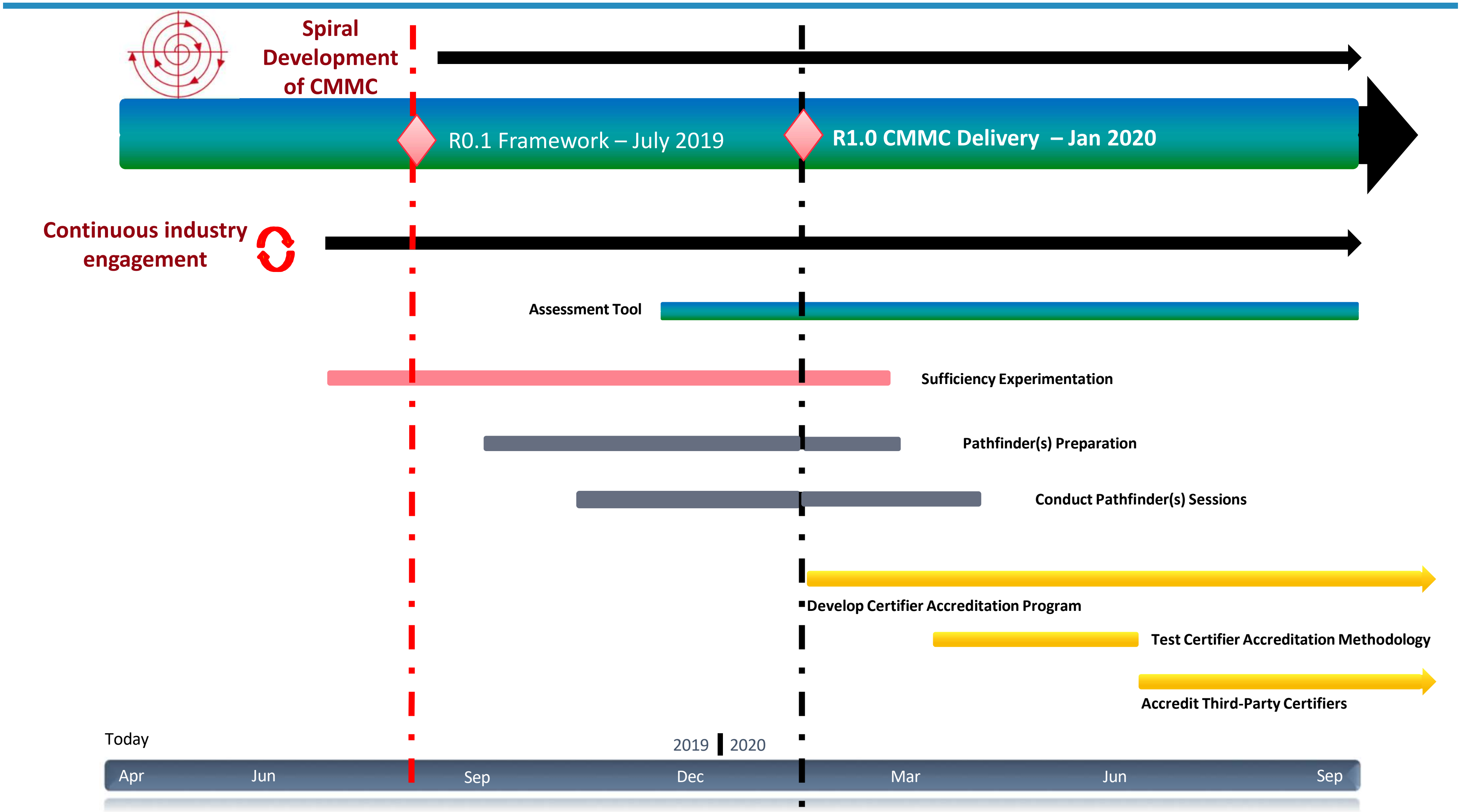
Certified Assessor Companies:

- Good business model at all levels
- Reasonable barrier to entry
- Similar or consistent with current evaluations

Model Developers:

- Logically consistent
- Meaningful, cumulative, "evenly spaced" levels
- Levels mapped to threat
- Comprehensive (all elements are addressed)
- Objective
- Measurable, feasible, and scalable

Notional CMMC Timeline



Spiral Development of CMMC

R0.1 Framework – July 2019

R1.0 CMMC Delivery – Jan 2020

Continuous industry engagement

Assessment Tool

Sufficiency Experimentation

Pathfinder(s) Preparation

Conduct Pathfinder(s) Sessions

Develop Certifier Accreditation Program

Test Certifier Accreditation Methodology

Accredit Third-Party Certifiers

Today

2019 | 2020

Apr Jun Sep Dec Mar Jun Sep

🟦 Task 1: Build and Refine CMMC

🟩 Task 2: Build and Refine CMMC

🟥 Task 3: Model Sufficiency Experimentation

⬛ Task 4: Conduct Model Pathfinder

🟨 Task 5: Build the Third-Party Accreditation Program

UNCLASSIFIED

Industry Days / Listening Sessions

We are looking at 11 collaborative sessions across the country and we want to ensure, we give all an equal voice for participation.

Time Frame: July – Aug 2019

Locations:

San Diego, CA
San Antonio, TX
Huntsville, AL
Tampa, FL
Boston, MA
Washington D.C.
Phoenix, AZ
Detroit, MI
Colorado Springs, CO
Seattle, WA
Kansas City, KA

Questions?

Katie Arrington, HQE Cyber for ASD (A)
Katherine.e.arrington.civ@mail.mil
703-695-9332