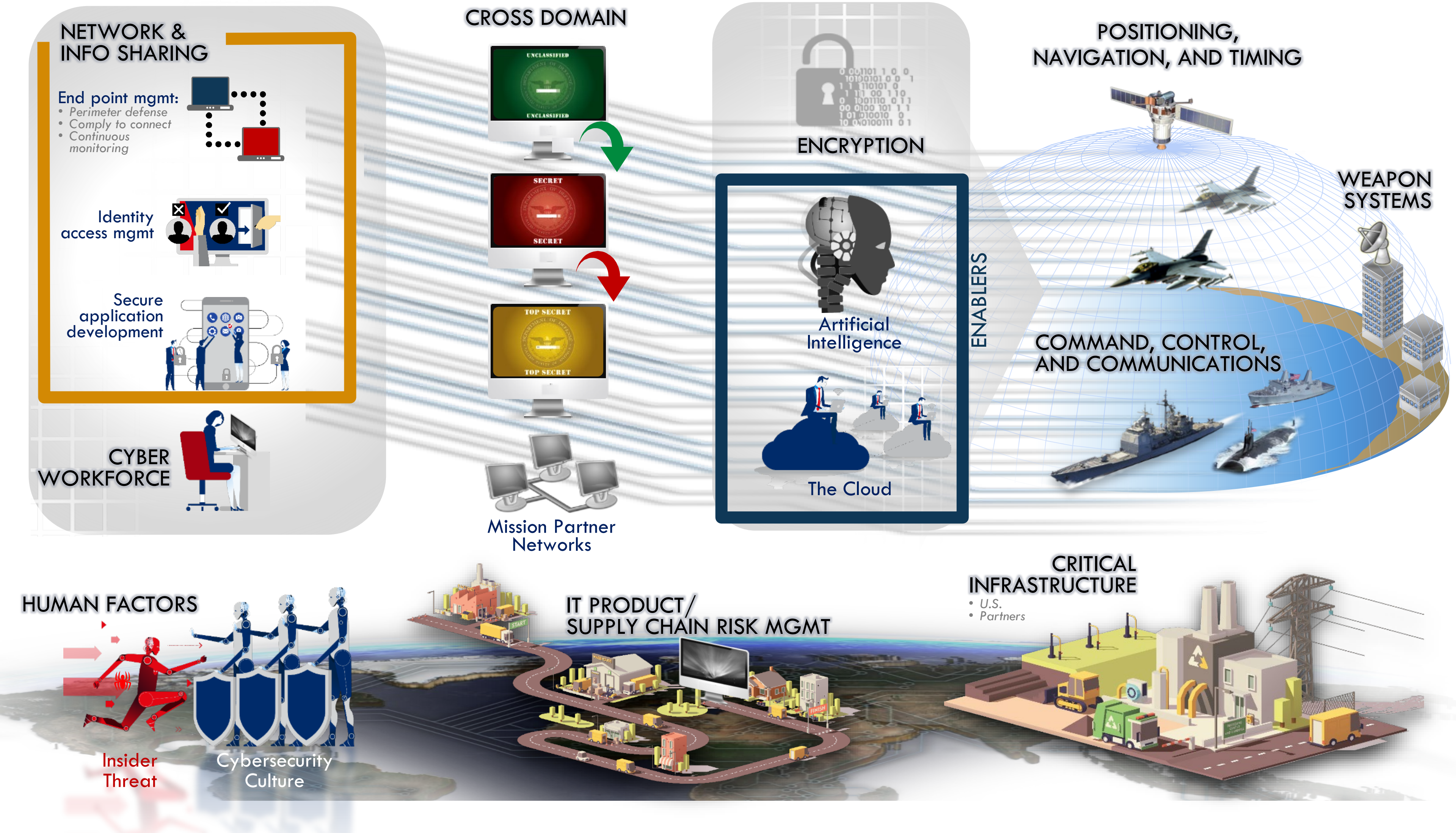
Cybersecurity Maturity Model Certification (CMMC)

Ms. Katie Arrington
HQE, Special Assistant for Cyber
OUSD(A&S)/ASD(A)

5 Jul 2019

Background: 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

Artificial Intelligence

The Cloud

ENABLERS

POSITIONING, NAVIGATION, AND TIMING

WEAPON SYSTEMS

COMMAND, CONTROL, AND COMMUNICATIONS

HUMAN FACTORS

Insider Threat

Cybersecurity Culture

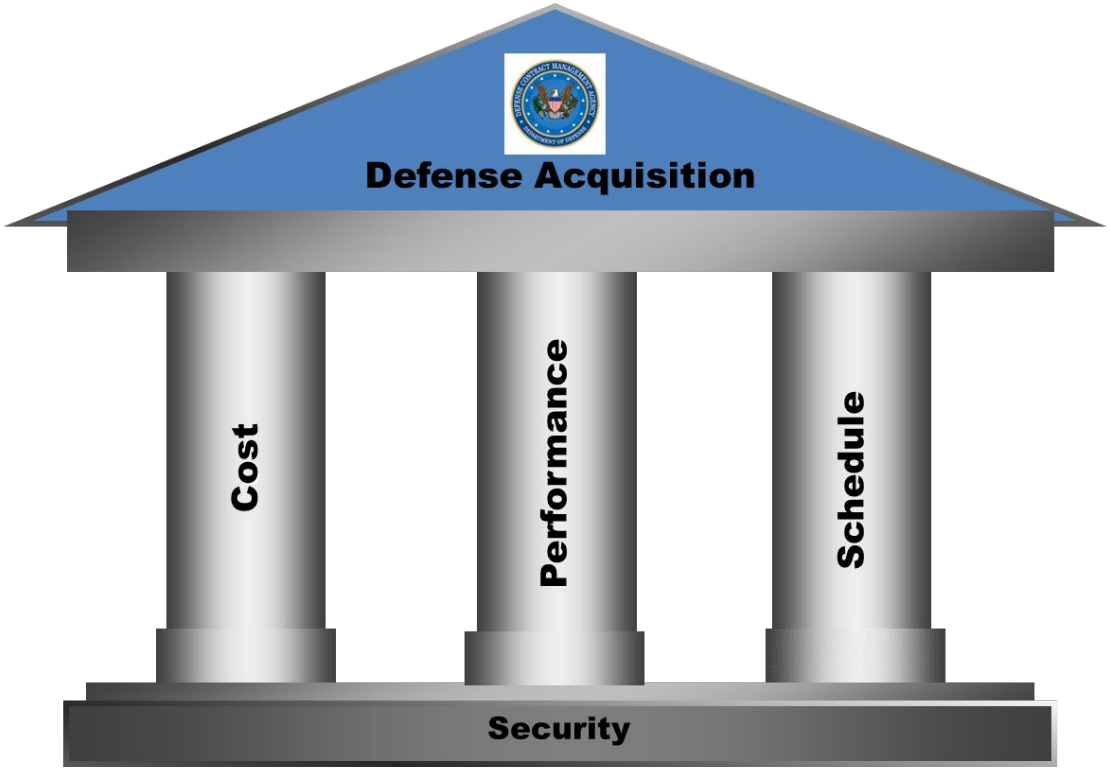
IT PRODUCT/ SUPPLY CHAIN RISK MGMT

CRITICAL INFRASTRUCTURE
- U.S.
- Partners

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

Cost, Schedule, Performance

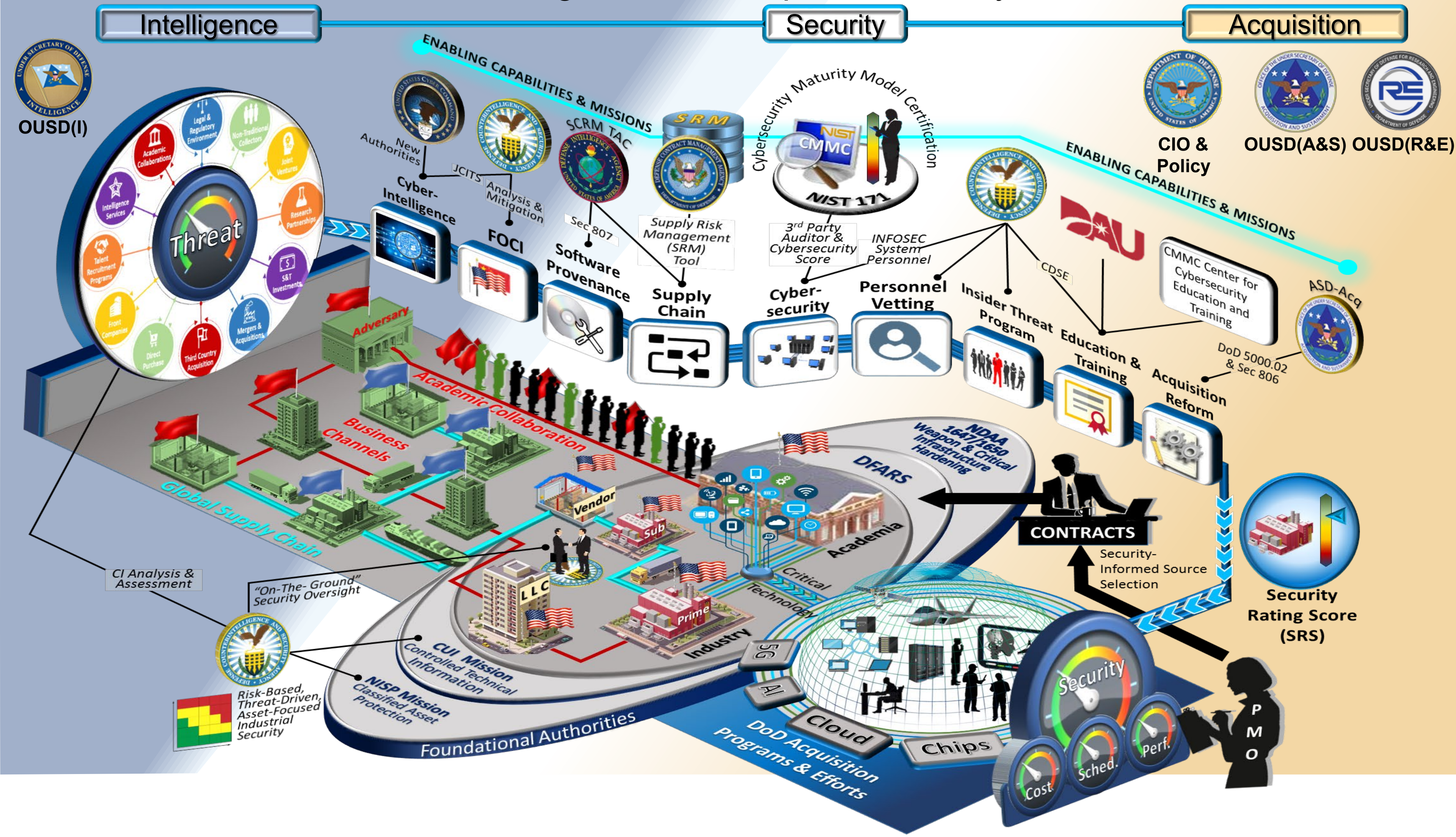
ARE ONLY EFFECTIVE IN A SECURE ENVIROMENT



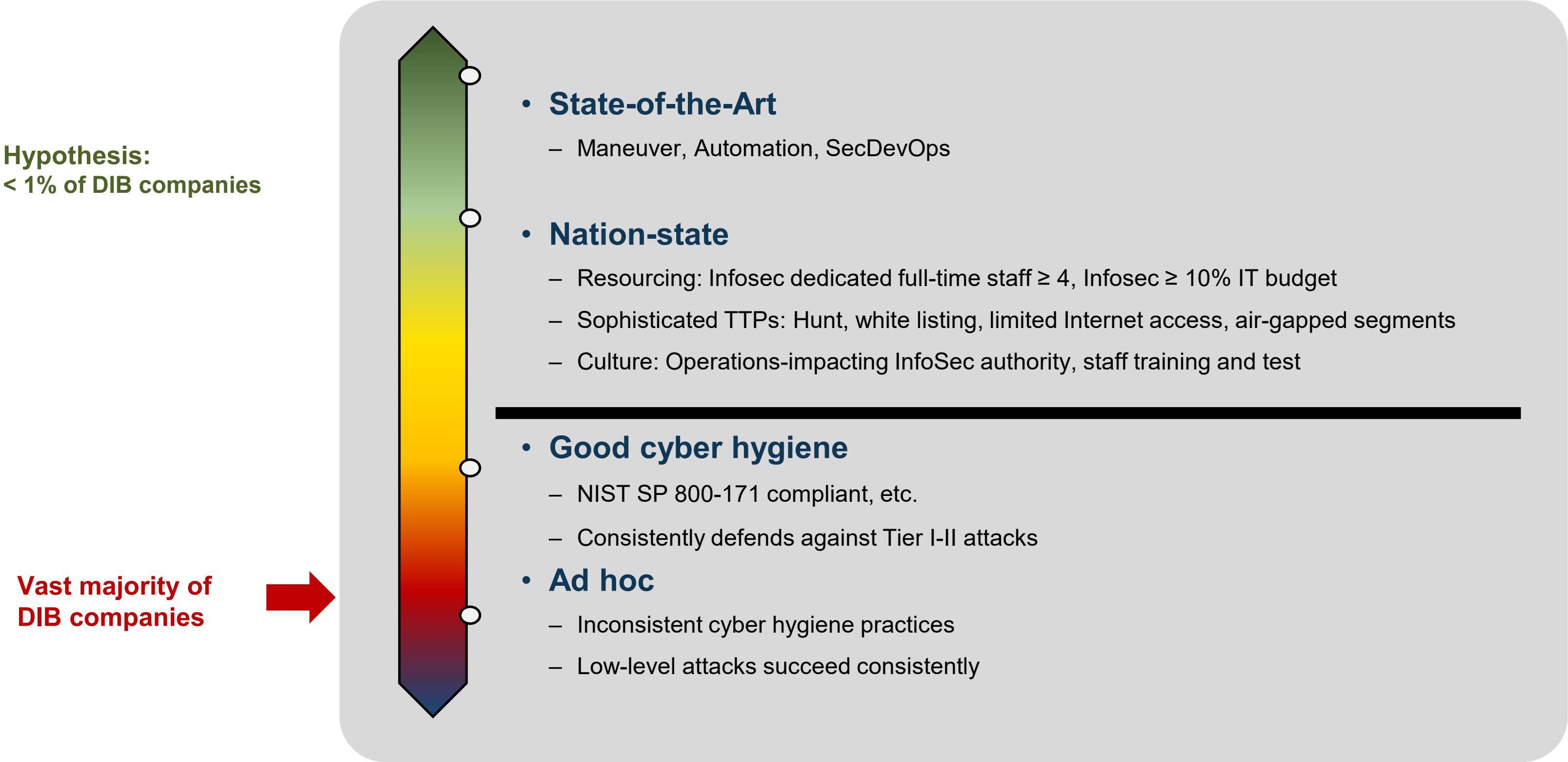
Cybersecurity Maturity Model Certification (CMMC)

- 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.

Securing the DoD Acquisition Ecosystem



DIB Cybersecurity Posture



Hypothesis:
< 1% of DIB companies

Vast majority of
DIB companies

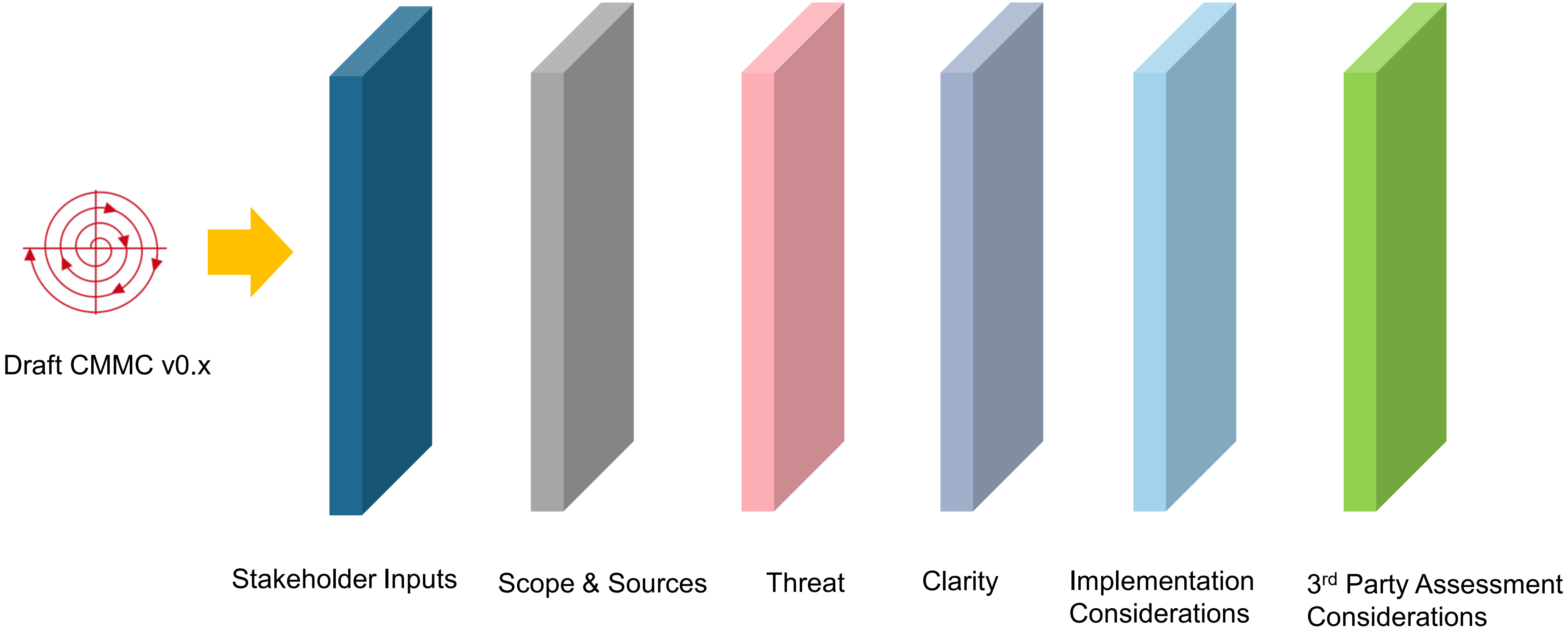
- **State-of-the-Art**
  - Maneuver, Automation, SecDevOps
- **Nation-state**
  - Resourcing: Infosec dedicated full-time staff ≥ 4, Infosec ≥ 10% IT budget
  - Sophisticated TTPs: Hunt, white listing, limited Internet access, air-gapped segments
  - Culture: Operations-impacting InfoSec authority, staff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

Notional CMMC Model Development

- **CMMC will be updated and revised in an iterative manner until Version 1.0 is delivered in Jan 2020**



Draft CMMC v0.x

Stakeholder Inputs

Scope & Sources

Threat

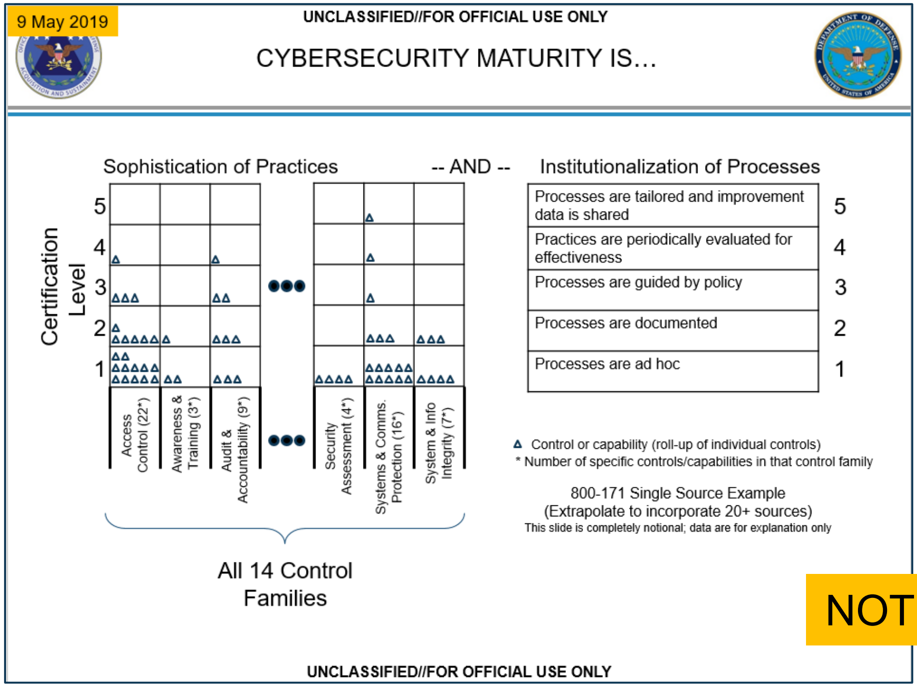
Clarity

Implementation Considerations

3rd Party Assessment Considerations

Development of CMMC will take into account multiple perspectives and considerations; each successive draft version will incorporate additional analyses and inputs

Notional CMMC Model



9 May 2019

UNCLASSIFIED//FOR OFFICIAL USE ONLY

CYBERSECURITY MATURITY IS…

Sophistication of Practices -- AND -- Institutionalization of Processes

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

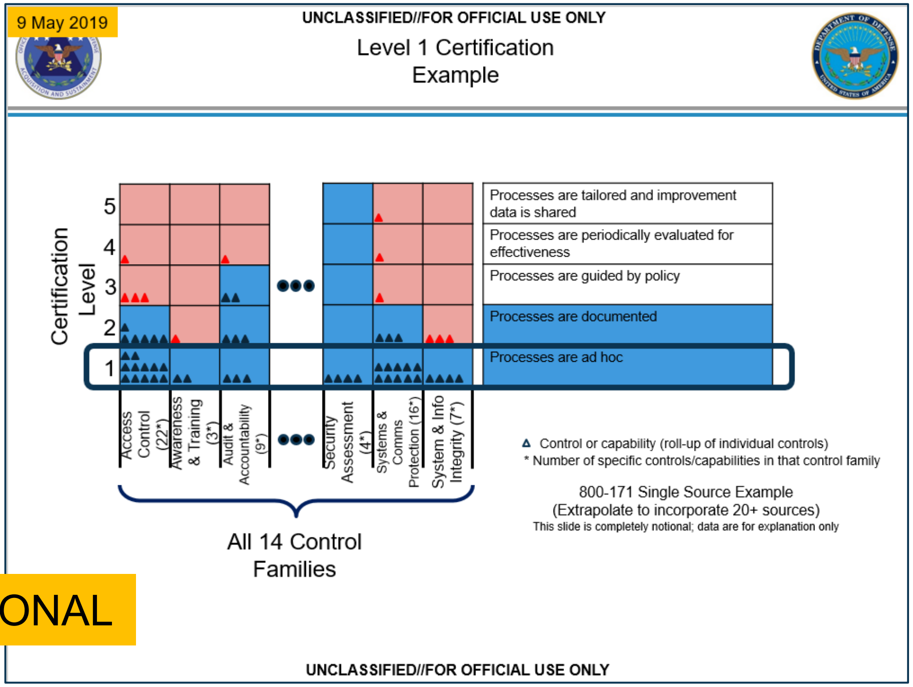
△ Control or capability (roll-up of individual controls)

* Number of specific controls/capabilities in that control family

800-171 Single Source Example
(Extrapolate to incorporate 20+ sources)

This slide is completely notional; data are for explanation only

UNCLASSIFIED//FOR OFFICIAL USE ONLY



9 May 2019

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Level 1 Certification Example

Certification Level
5
4
3
2
1
Access Control (22*)
Awareness & Training (3*)
Audit & Accountability (9*)
Security Assessment (4*)
Systems & Comms Protection (16*)
System & Info Integrity (7*)
All 14 Control Families

Processes are tailored and improvement data is shared
Processes are periodically evaluated for effectiveness
Processes are guided by policy
Processes are documented
Processes are ad hoc

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

* Number of specific controls/capabilities in that control family

800-171 Single Source Example
(Extrapolate to incorporate 20+ sources)

This slide is completely notional; data are for explanation only

UNCLASSIFIED//FOR OFFICIAL USE ONLY

NOTIONAL

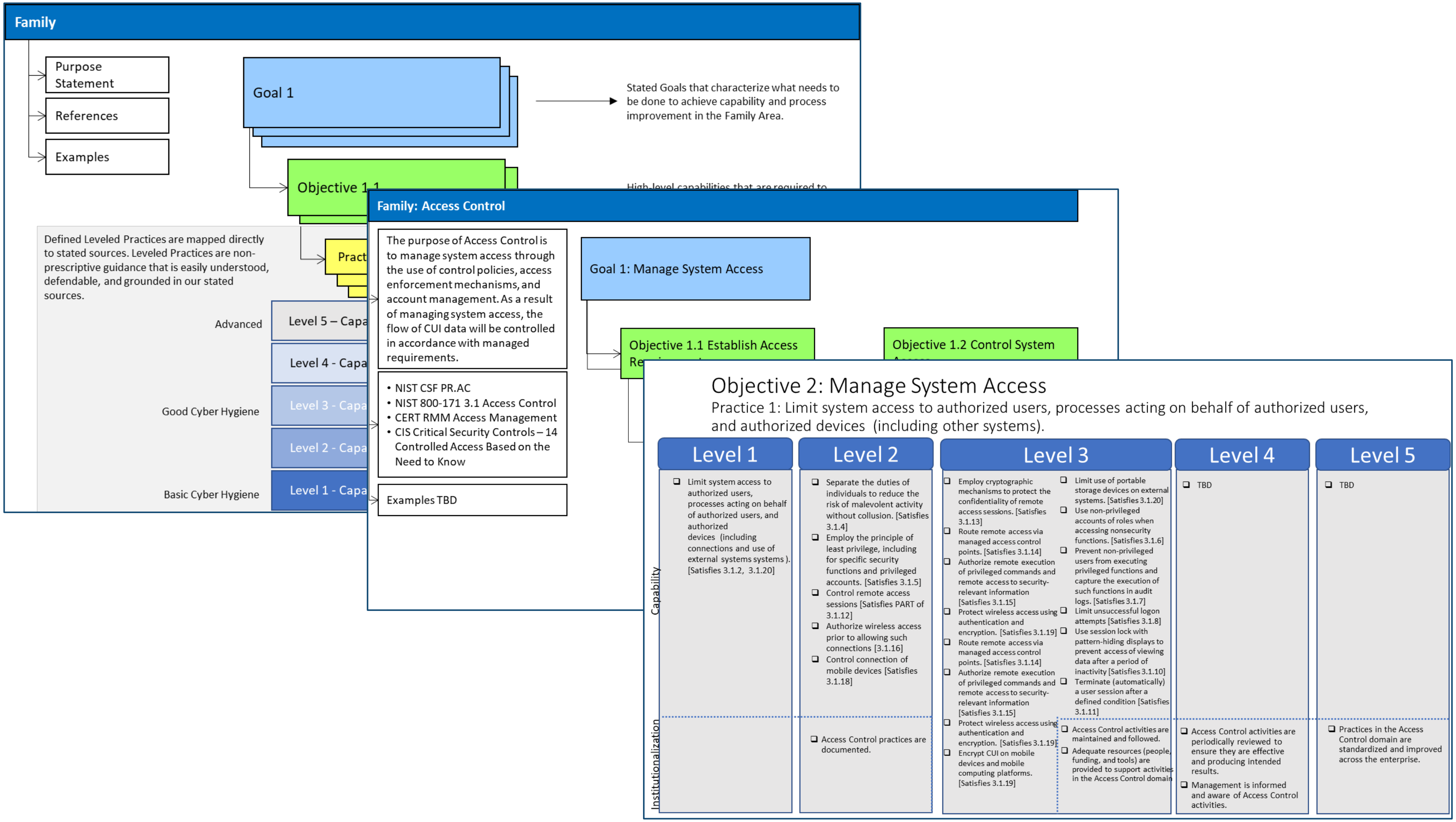
CMMC will measure cybersecurity maturity by the implementation of practices and institutionalization of processes

Draft CMMC Model v0.2

	Initial Thinking	Initial Mapping: Practices (Controls)	Initial Mapping: Processes
CMMC Level 5	Advanced / Progressive	Draft NIST SP 800-171B	CMM derived sources (pending)
CMMC Level 4	Proactive		
CMMC Level 3	Good Cyber Hygiene	NIST SP 800-171 rev1 Additional references reviewed: • DIB SCC TF WG Top 10 • AIA NAS 9933 • UK Cyber Essentials • AUS Essential Eight • Other	
CMMC Level 2	Intermediate Cyber Hygiene		
CMMC Level 1	Basic Cyber Hygiene		

The draft CMMC model will continue to evolve and improve based on inputs and joint work with industry and DoD stakeholders

Draft CMMC v0.2: Example of Details



Family

Purpose Statement

References

Examples

Goal 1

Stated Goals that characterize what needs to be done to achieve capability and process improvement in the Family Area.

Objective 1.1

High-level capabilities that are required to

Defined Leveled Practices are mapped directly to stated sources. Leveled Practices are non-prescriptive guidance that is easily understood, defendable, and grounded in our stated sources.

Pract

Advanced

Level 5 – Capa

Level 4 - Capa

Good Cyber Hygiene

Level 3 - Capa

Level 2 - Capa

Basic Cyber Hygiene

Level 1 - Capa

Family: Access Control

The purpose of Access Control is to manage system access through the use of control policies, access enforcement mechanisms, and account management. As a result of managing system access, the flow of CUI data will be controlled in accordance with managed requirements.

- NIST CSF PR.AC
- NIST 800-171 3.1 Access Control
- CERT RMM Access Management
- CIS Critical Security Controls – 14 Controlled Access Based on the Need to Know

Examples TBD

Goal 1: Manage System Access

Objective 1.1 Establish Access Re

Objective 1.2 Control System

Objective 2: Manage System Access

Practice 1: Limit system access to authorized users, processes acting on behalf of authorized users, and authorized devices (including other systems).

	Level 1	Level 2	Level 3	Level 4	Level 5
Capability	❑ Limit system access to authorized users, processes acting on behalf of authorized users, and authorized devices (including connections and use of external systems systems). [Satisfies 3.1.2, 3.1.20]	❑ Separate the duties of individuals to reduce the risk of malevolent activity without collusion. [Satisfies 3.1.4] ❑ Employ the principle of least privilege, including for specific security functions and privileged accounts. [Satisfies 3.1.5] ❑ Control remote access sessions [Satisfies PART of 3.1.12] ❑ Authorize wireless access prior to allowing such connections [3.1.16] ❑ Control connection of mobile devices [Satisfies 3.1.18]	❑ Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. [Satisfies 3.1.13] ❑ Route remote access via managed access control points. [Satisfies 3.1.14] ❑ Authorize remote execution of privileged commands and remote access to security-relevant information [Satisfies 3.1.15] ❑ Protect wireless access using authentication and encryption. [Satisfies 3.1.19] ❑ Route remote access via managed access control points. [Satisfies 3.1.14] ❑ Authorize remote execution of privileged commands and remote access to security-relevant information [Satisfies 3.1.15] ❑ Protect wireless access using authentication and encryption. [Satisfies 3.1.19] ❑ Encrypt CUI on mobile devices and mobile computing platforms. [Satisfies 3.1.19] ❑ Limit use of portable storage devices on external systems. [Satisfies 3.1.20] ❑ Use non-privileged accounts of roles when accessing nonsecurity functions. [Satisfies 3.1.6] ❑ Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. [Satisfies 3.1.7] ❑ Limit unsuccessful logon attempts [Satisfies 3.1.8] ❑ Use session lock with pattern-hiding displays to prevent access of viewing data after a period of inactivity [Satisfies 3.1.10] ❑ Terminate (automatically) a user session after a defined condition [Satisfies 3.1.11]	❑ TBD	❑ TBD
Institutionalization		❑ Access Control practices are documented.	❑ Access Control activities are maintained and followed. ❑ Adequate resources (people, funding, and tools) are provided to support activities in the Access Control domain	❑ Access Control activities are periodically reviewed to ensure they are effective and producing intended results. ❑ Management is informed and aware of Access Control activities.	❑ Practices in the Access Control domain are standardized and improved across the enterprise.

Near-term Meetings and Projected Milestones

Near-term meetings:

- [15-17 Jul] CMMC “Deep Dive” with subset of industry (i.e. Joint CMMC Working Group in concert with Defense Industrial Base Sector Coordinating Council Supply Chain Task Force WG)
- [24-26 Jul] CMMC Listening Tour: NDIA Navy Gold Coast Event

Projected milestones:

- [Jul – Sep 2019] CMMC Listening Tour
- [Fall 2019] Start initial pathfinders
- [Jan 2020] Complete CMMC Framework v1.0
- [Jan – Jun 2020] Training of 3rd party assessment organizations for CMMC
- [Jun 2020] CMMC to start appearing in RFIs
- [Sep 2020] CMMC to start appearing in RFPs

OUSD(A&S) is committed to building upon progress made in the Joint CMMC Working Group and continuing to work with industry and DoD stakeholders

SAM: Shared Assessment Model

Backups

CMMC Phase 1 Model v0.2 Alternate Source Mapping

- Reviewed six alternate sources to assess gaps and current levels in CMMC
  - Most sources examined map to a subset of CMMC Phase 1 Model v0.2 Levels 1-3
- Identified some gaps between sources and CMMC Phase 1 Model v0.2:
  - AIA NAS 9933 requires integrity and availability
    - Of the 68 controls not currently covered, all but 10 controls overlap with NIST SP 800-53
  - AUS Essential Eight requires daily backups; this is considered beyond the scope of CMMC

Number of Unique CMMC Phase 1 v0.2 Controls Mapped by Alternate Sources

Source Reviewed	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	No map to NIST SP 800-171
FAR 52.204-21	17	-	-	-	-	-
UK Cyber Essentials	5	6	6	-	-	-
Australia Essential Eight	3	-	4	-	-	1
AIA NAS 9933	11	23	22	?	?	68
DIB Top Ten	10	9	7	-	-	-
DoD CIO Scoring	Scores priorities across 800-171 instead of leveling; provides no new controls					