CNSS Supply Chain Risk Management Sub-Working Group (CNSS SCRM SWG)
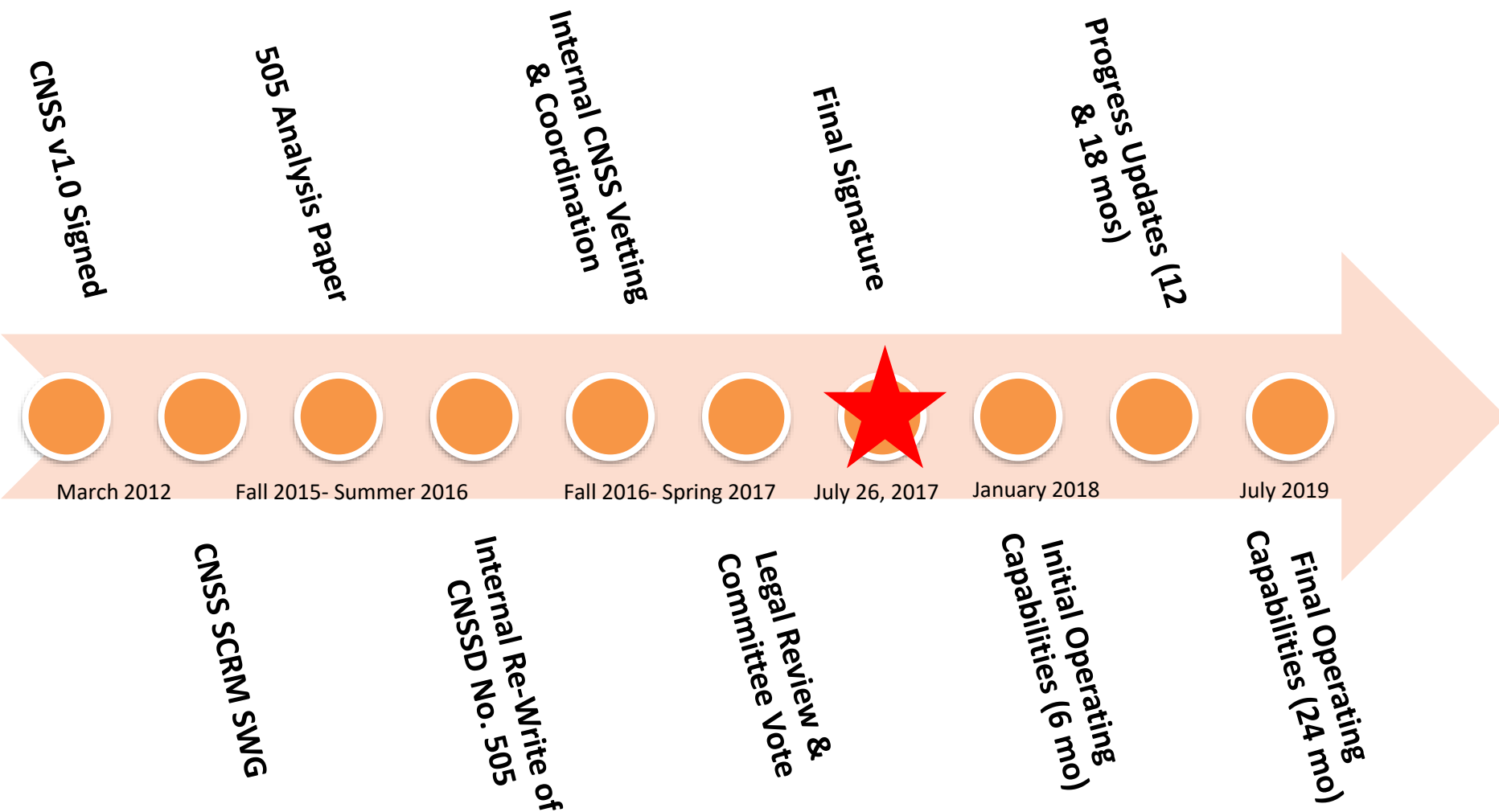
August 29, 2017
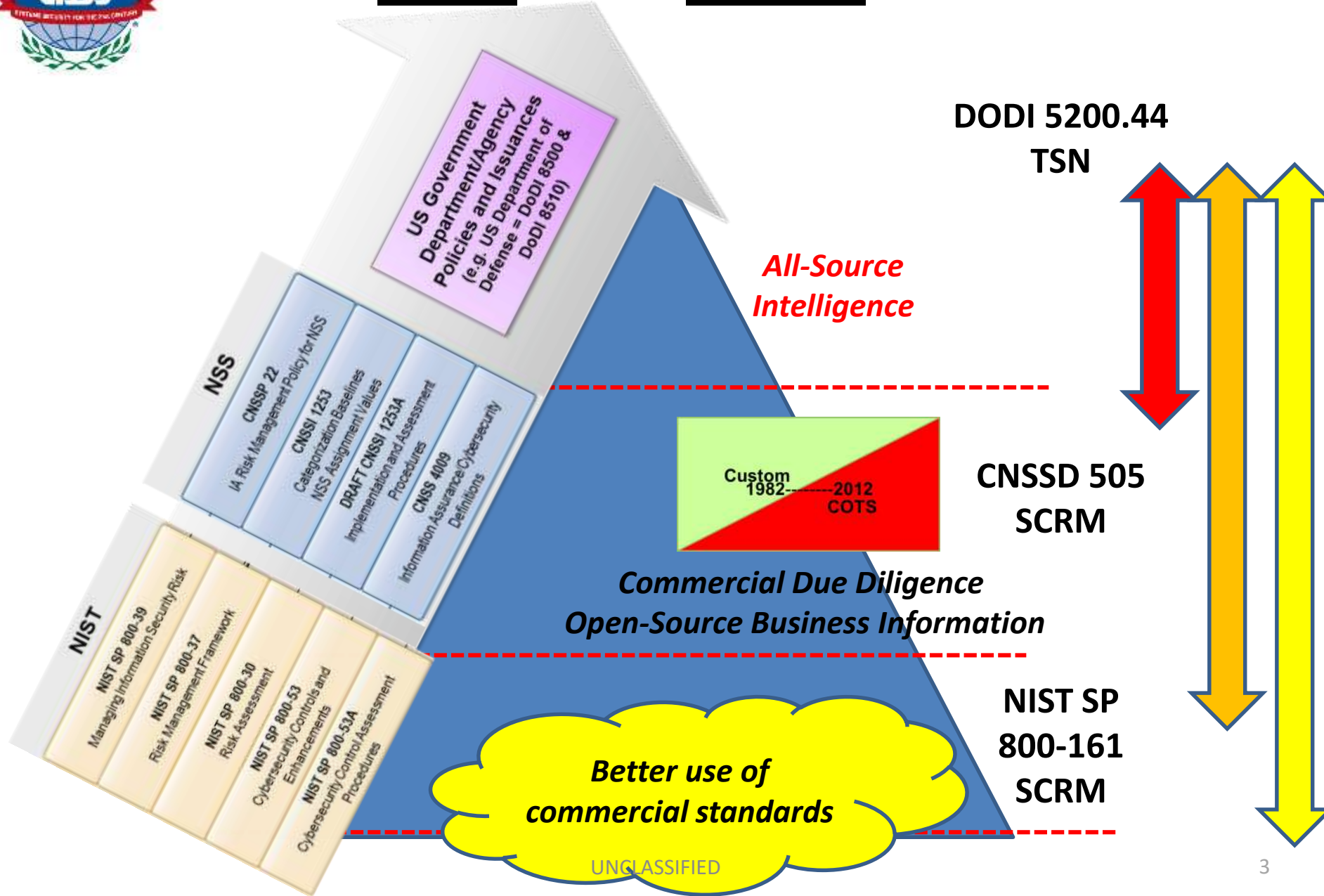
CNSSD No. 505
Implementation Timeline

CNSS v1.0 Signed

505 Analysis Paper

Internal CNSS Vetting & Coordination

Final Signature

Progress Updates (12 & 18 mos)

March 2012

Fall 2015- Summer 2016

Fall 2016- Spring 2017

July 26, 2017

January 2018

July 2019

CNSS SCRM SWG

Internal Re-Write of CNSSD No. 505

Legal Review & Committee Vote

Initial Operating Capabilities (6 mo)

Final Operating Capabilities (24 mo)

RMF & SCRM

US Government Department/Agency Policies and Issuances (e.g. US Department of Defense = DoDI 8500 & DoDI 8510)

NSS
- CNSSP 22 — IA Risk Management Policy for NSS
- CNSSI 1253 — Categorization Baselines NSS Assignment Values
- DRAFT CNSSI 1253A — Implementation and Assessment Procedures
- CNSS 4009 — Information Assurance/Cybersecurity Definitions

NIST
- NIST SP 800-39 — Managing Information Security Risk
- NIST SP 800-37 — Risk Management Framework
- NIST SP 800-30 — Risk Assessment
- NIST SP 800-53 — Cybersecurity Controls and Enhancements
- NIST SP 800-53A — Cybersecurity Control Assessment Procedures

DODI 5200.44 TSN

All-Source Intelligence

Custom 1982 -------- 2012 COTS

CNSSD 505 SCRM

Commercial Due Diligence Open-Source Business Information

NIST SP 800-161 SCRM

Better use of commercial standards

What Changed?

- CNSSD 505
  - Enabled sharing of the policy across the SCRM Community (no longer an FOUO document)
  - Updated out of date references and authorities related to SCRM (to include software assurance, hardware assurance / anti-counterfeits, and assured services)
  - Transition to Risk Management Framework (RMF) and management of lifecycle cybersecurity
  - The relationship and dependencies of national security capabilities on non-national security systems

- Established a sub-working group under CNSS Safeguarding Working Group to:
  - Engage broader SCRM efforts and experts, promote information sharing, improve visibility across the CNSS community.
  - Remain current with developments in the field of SCRM, current policy, and emerging activities.
  - Monitor and provide feedback on the maturing capabilities and implementation of CNSSD 505

Initial Operating Capability – Quad Chart

DRAFT

Primary POC: Name, email
Alternate POC (if applicable): Name, email
GO/SES (if applicable):
Contractor support (if applicable):

Purpose: Brief statement describing your mission statement with respect to CNSSD No. 505 on Supply Chain Risk Management
Scope: Focus / Limits of your program; lanes in the road (if applicable- not same as Issues below)

Current Activities (On-Going):
- Helpful to include a metric to show progress (i.e.: timeline to completion, bullets to show action is either in the works, ongoing, and completed, etc.)
- Include CNSS instruction, if applicable

Items Completed/Accomplishments:
- Planning meetings (& frequency)
- Collaboration efforts throughout the community.
- Goals achieved
- Include pursing policies or published policies, guidebooks, surveys, etc.
- Include CNSS instruction, if applicable

Issues:
- List any obstacles/stumbling blocks
- What help do you need from the CNSS (or higher) to assist you in resolving these issues?
- Hurdles hindering your success in meeting CNSSD No. 505 Requirements

Status *(Delete this box after selecting stoplights below):*
Take a look at your organizational responsibilities as defined in CNSSD No. 505. Are you on schedule to provide all by the end of FY18? Give a status of your org for each of the 8 responsibilities (current & FY18). See next slide for stoplight examples to copy/paste and match with 505 responsibility.

SCRM Implementation Status based CNSSD No. 505 – Initial Operating Capabilities (6 mos.)   FOC 8/2019

V.11.a.i.1: *Identify and designate a SCRM POC.*

POC

V.11.a.ii

V.11.a.i.2: *Provide for participation in CNSS SCRM activities to the fullest extent possible.*

V.11.a.i.3: Develop and obtain approval of a SCRM strategy and implementation plan. The strategy and implementation plan should include guidance for the evolution and sustainment of the department or agency-specific SCRM capability for NSS.

Assess	Requirements	Prioritize	Life Cycle	Contracting	Document
V.11.a.i	V.11.a.iii	V.11.a.v	V.11.a.vi	V.11.a.vii	V.11.a.ix

UNCLASSIFIED
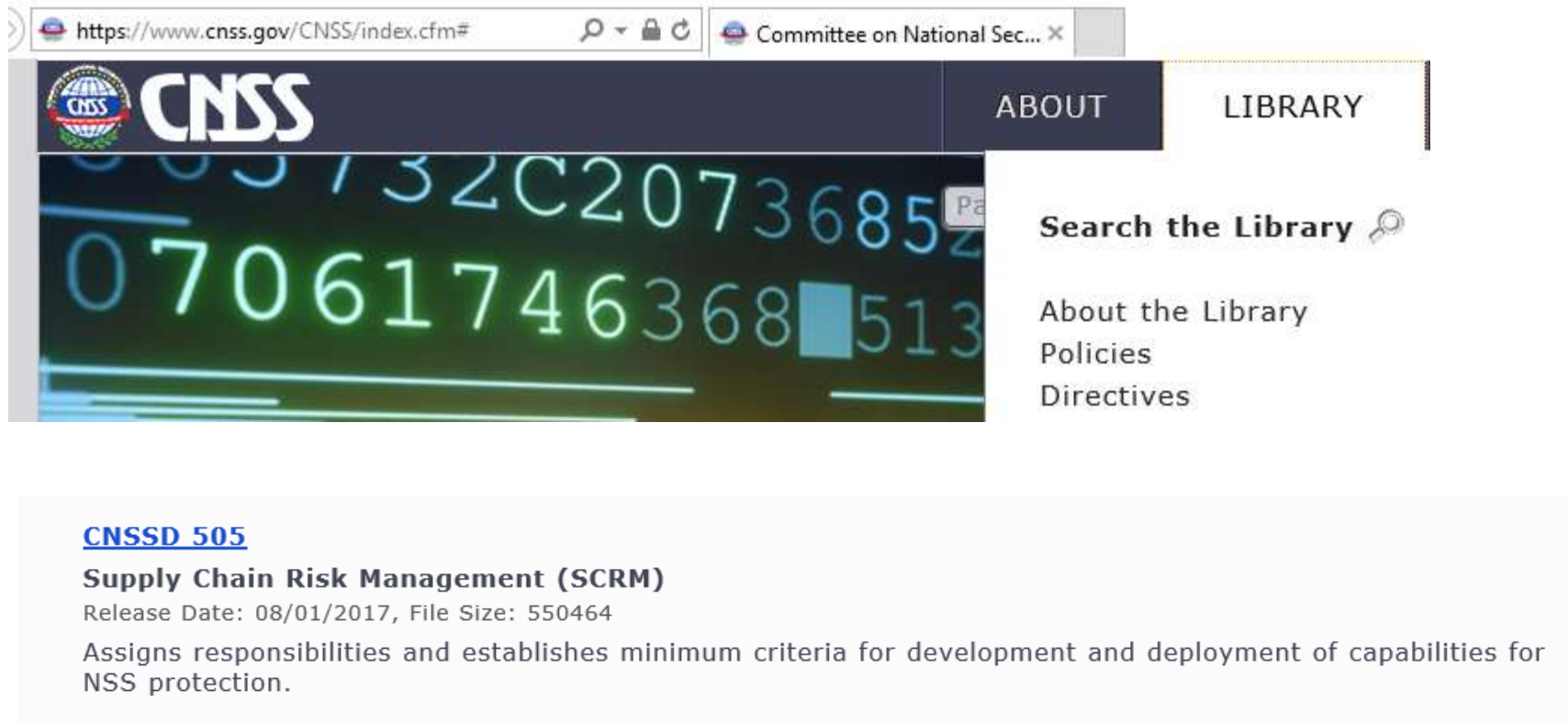
CNSSD 505 Signed August 2017

CNSSD 505

Supply Chain Risk Management (SCRM)

Release Date: 08/01/2017, File Size: 550464

Assigns responsibilities and establishes minimum criteria for development and deployment of capabilities for NSS protection.