Secure by Standards

ON THE ACCEPTABLE USE OF COMMERCIAL STANDARDS IN FEDERAL IT ACQUISITIONS

Commercial Standards and Federal IT Acquisitions

- The Common Call
- What are Commercial Standards?
- Commercial Standards Organizations
- Government's Use of Commercial Standards
- Common Commercial Standards
- Conclusion, Considerations, Challenges

Commercial Standards Advocacy:

- Legislative Branch
- Executive Branch
- Bi-Partisan

The Common Call

The Common Call Continued

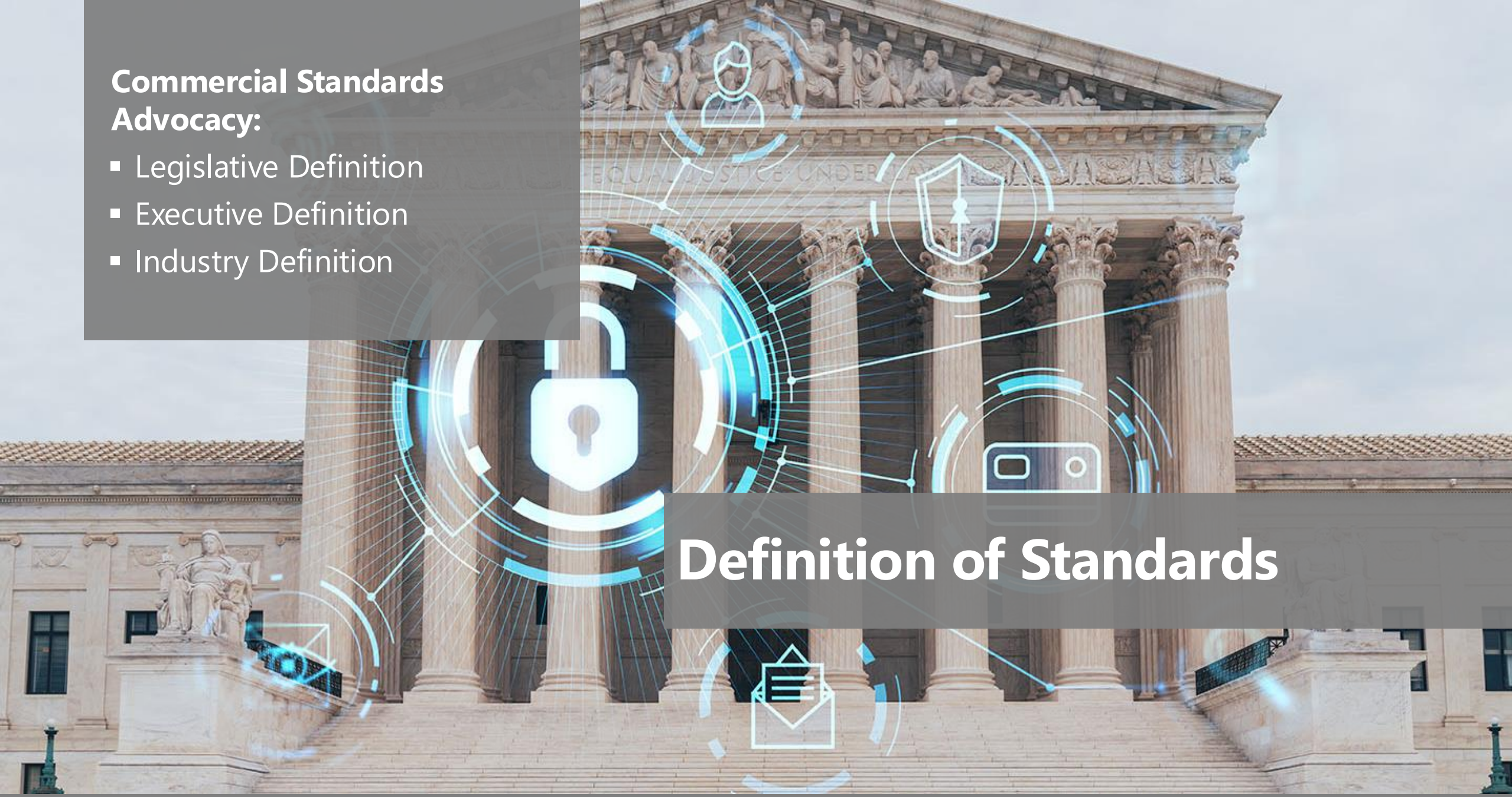
Commercial Standard References

In 1977 Congress defined Commercial Standard in 15 U.S. Code § 788.

The 1995 Technology Transfer Act defined NIST's role in standards conformity. The law was amended to include public law "Utilization of Consensus Technical Standards by Federal Agencies" in 2001.

In 2023 the Biden Administration released the "National Standards Strategy for Critical and Emerging Technology."

- "All federal agencies must use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical." - OMB Circular NO. A-119
- "In these circumstances, your agency must submit a report describing the reason(s) for its use of government-unique standards in lieu of voluntary consensus standards to the Office of Management and Budget (OMB) through the National Institute of Standards and Technology (NIST)." - OMB Circular NO. A-119
- "When possible and appropriate, acquirers should allow [industry] the opportunity to reuse applicable existing data and documentation that may provide evidence to support C-SCRM (e.g., certification of a vendor to a relevant standard, such as ISO 27001). *Doing this results in cost savings to the acquirer and supplier*." – NIST 800-161



Commercial Standards Advocacy:

- Legislative Definition
- Executive Definition
- Industry Definition

Definition of Standards

Definition of Commercial Standards

Legislative Branch Definition

Commercial Standards contain:

1. Specifications of materials;
2. Methods of testing;
3. Criteria for adequate performance or operations;
4. Model codes;
5. Classification of components;
6. Delineation of procedures or definition of terms;
7. Quantitative or qualitative measurements for evaluation;
8. Similar rules, procedures, requirements, or standards

Executive Branch Definition

"Standards are essential to commerce, allowing technology to work seamlessly and business to operate smoothly. They provide industries and innovators with a common language that facilitates trade, simplifies transactions, and enables people to work together toward greater common goals that cut across disciplines and borders."

Industry Definition

Commercial Standards are technical standards organized by a standards organization whose work is to create consensus between companies, stakeholders, and other interested parties that result in the development, coordination, release, and update of a specific technical standard.

Standards Organizations

- The Big Three
- Other Standards Organizations

International Standards Organizations

International Organization for Standardization (ISO)

International Electrotechnical Commission (IEC)

International Telecommunications Union (ITU)

More Standards Organizations

The Open Group

Institute of Electrical and Electronic Engineers (IEEE)

American National Standards Institute

Standards Creation and Adoption
Legislative Branch
Executive Branch
Department of Defense
NIST
Other Agencies

Government-wide Agreements
NASA SEWP
General Services Administration
NITAAC

Agency Acquisitions
NASA
USAF
Department of Energy
Other Federal Agencies

Government Use of Commercial Standards

Common Commercial Standards & Other Approaches

- ISO/IEC 9001
- ISO/IEC 20000
- ISO/IEC 20243
- ISO/IEC 27001
- ISO/IEC 27036
- CMMI
- CMMC

ISO 9001 – Quality Management

The ISO 9001 standard specifies requirements for the establishment, maintenance, and continuous improvement of a **quality management** system, covering a wide range of topics including:

Organizational Context	**Leadership**	**Planning**
Support	**Operation**	**Performance Evaluation**
	Continuous Improvement	

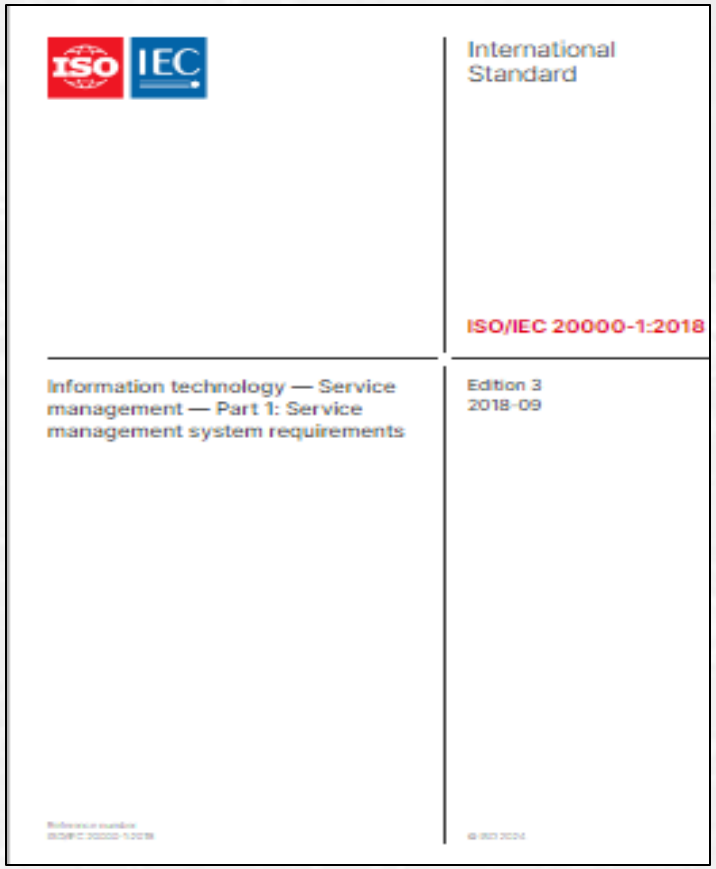
ISO/IEC 20000 — IT Service management

This standard specifies requirements for an organization to establish, implement, maintain and continually improve a service management system (SMS).

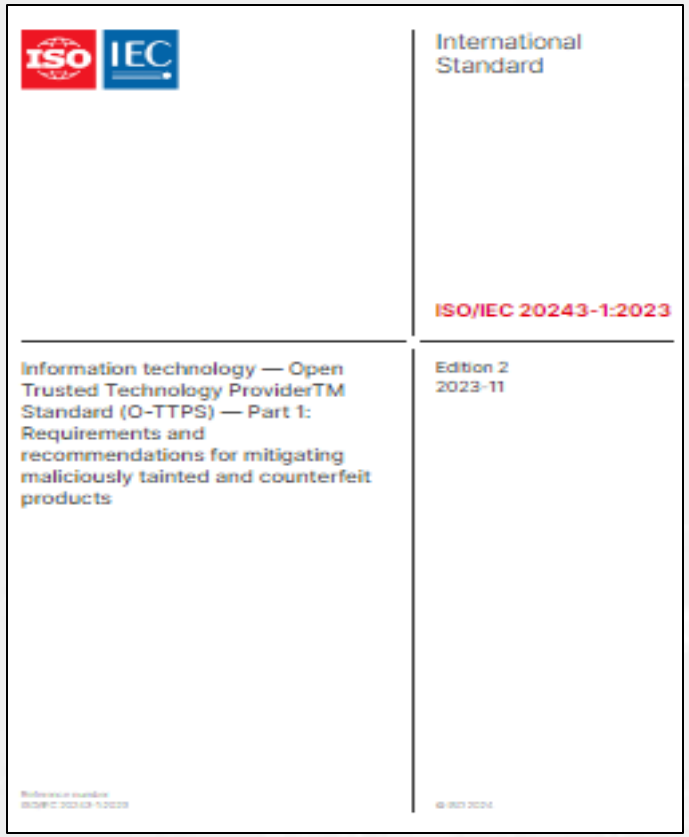
The requirements specified in this standard include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value.

Standard is used for:

Service Assurance	Consistency	Capability Demonstration
Monitoring and Measurement	**Continuous Improvement**	**Requirements-based Assessments**
	Service Management Training	



ISO/IEC 20243 — Open Trusted Technology Provider Standard


ISO IEC

International Standard

ISO/IEC 20243-1:2023

Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products

Edition 2
2023-11

ISO/IEC 20243-1:2018 (O-TTPS) is a set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software COTS ICT products throughout the product life cycle. This release of the Standard addresses threats related to maliciously tainted and counterfeit products.

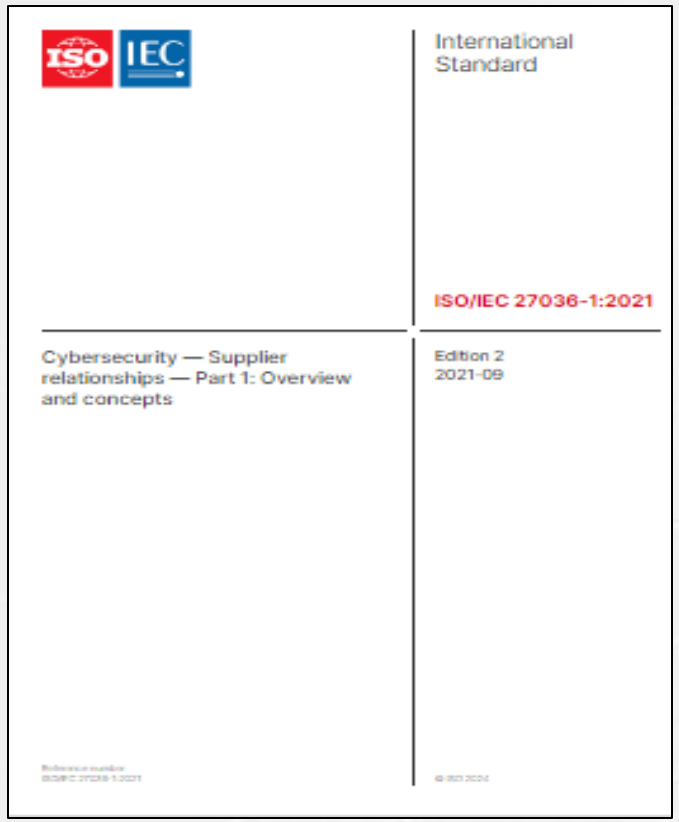
The provider's product life cycle includes the work it does designing and developing products, as well as the supply chain aspects of that life cycle, collectively extending through the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

ISO/IEC 27001 — Information security, cybersecurity and privacy protection

ISO/IEC 27001 The ISO/IEC 27001 standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

This standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

ISO/IEC 27036 — Cybersecurity — Supplier relationships



ISO/IEC 27036 is a standard that specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.

It covers any procurement and supply of products and services, such as manufacturing or assembly, business process procurement, software and hardware components, knowledge process procurement, build-operate-transfer and cloud computing services.

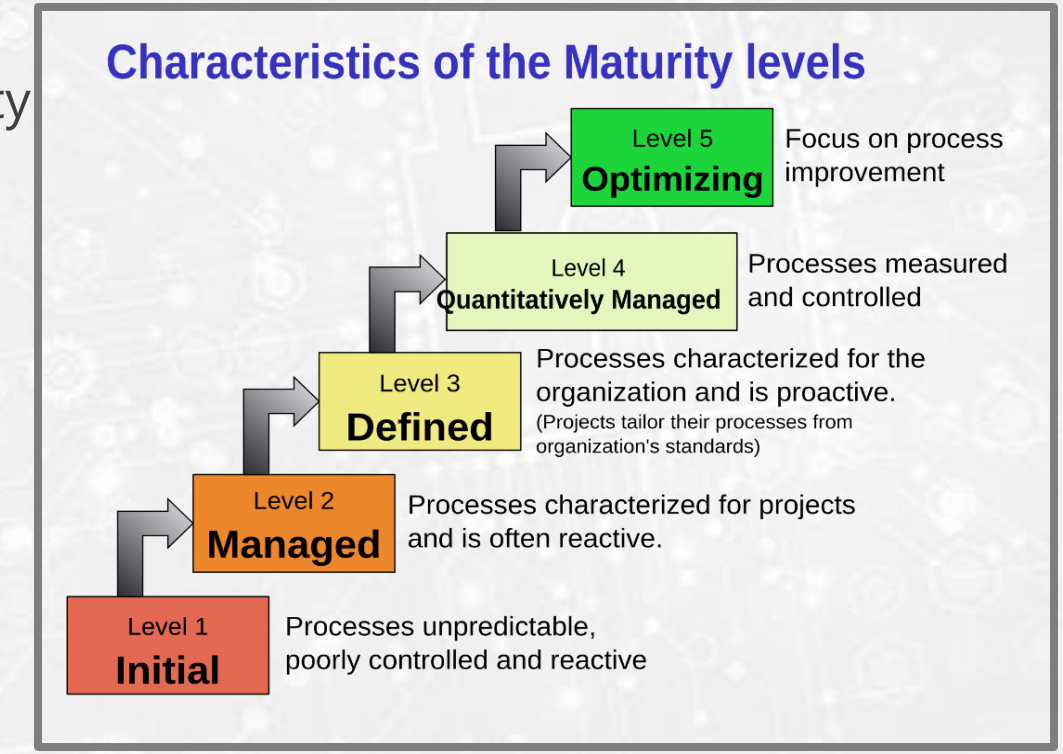
Companies who meet this standard has, as an organization, internally implemented several foundational processes including: business management, risk management, operational and human resources management, and information security.

CMMI Institute & Capability Maturity Model Integration (CMMI)

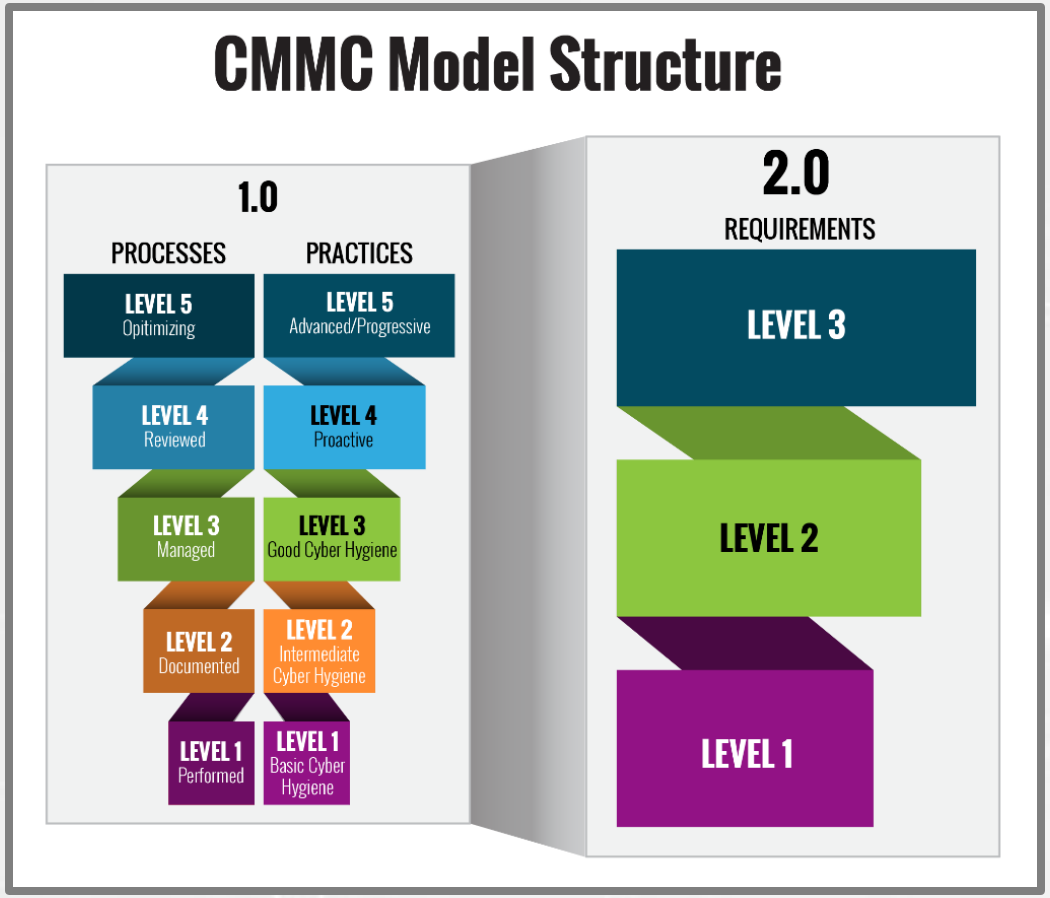
- A model, not a standard.
- CMMI assessments are required for software development contracts in the DOD, NASA, and throughout the federal government.
- CMMI began with the DOD and Carnegie Mellon University
- CMMI is managed by the CMMI Institute

It defines five maturity levels (1 to 5) for processes: Initial, Managed, Defined, Quantitatively Managed, and Optimizing.

Companies seeking to prove out their capabilities need to show how their organizational practices meet the highest level of maturity in their software development practices.



Cybersecurity Maturity Model Certification & The Cyber AB



- An emergent program closely modeled off CMMI
- Currently an initiative in transition.
- Accreditation body is the Cyber AB (formerly the CMMC Advisory Board)

Companies seeking this credential have their practices assessed against what is required of the industry in NIST SP 800-171. "To satisfy Under CMMC 2.0, the "Advanced" level (Level 2) will be equivalent to the NIST SP 800-171. The "Expert" level (Level 3), which is *currently under development*, will be based on a subset of NIST SP 800-172 requirements."

Conclusion, Considerations, Challenges

The Federal government has invested in the creation, use, and adoption of commercial standards

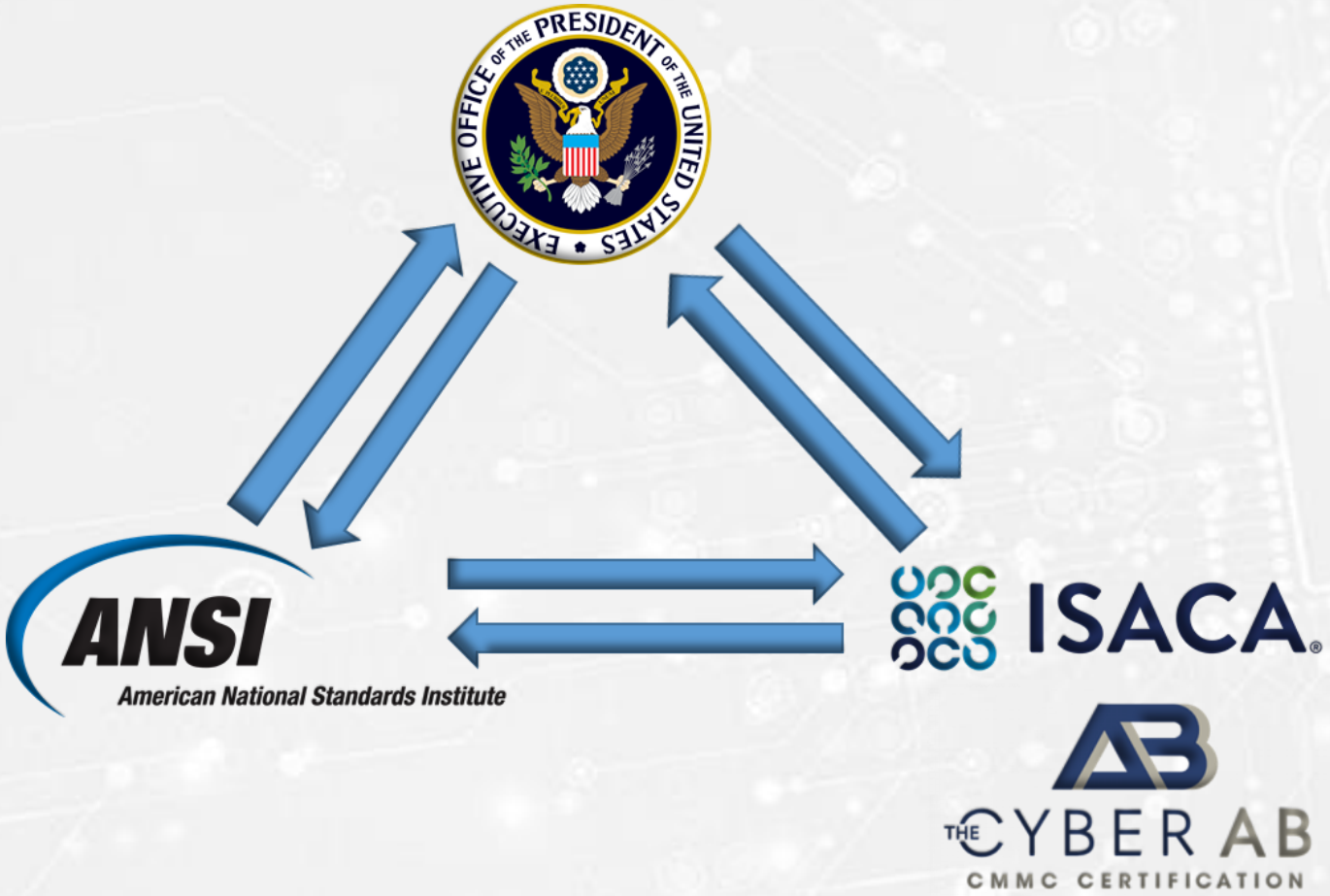
Commercial standards are a foundation for government guidance, or in requirements, when procuring ITC.

It is important to know about these standards, understand where they come from, and what is required of companies.

Government should seek ways to reduce the burden place onto industry through reciprocity.

The challenges in doing so are real.

Conclusion, Considerations, Challenges Continued



For more information

Standards Crosswalk I

https://tinyurl.com/3npbw8w6

Standards Crosswalk II

https://tinyurl.com/e9vhwduu

Govt. Use of Commercial Standards

https://tinyurl.com/4jnta7hu

Thank You!

Thank you to our many colleagues in government and industry who contributed to this topic with a particular emphasis on the supply chain risk management and cybersecurity community (in particular NIST, CISA, and our federal colleagues in “The Exchange”). Thank you to the NASA ITPO for providing the leadership, oversight, and support of the most impactful IT Acquisition vehicle in the federal government. Thank you to the NASA SEWP program for continuing to be a brain and a bridge that connects the federal government and industry.