NASA SEWP

Solutions for Enterprise-Wide Procurement

SECURITY STANDARDS

Title: Secure-by-Standards: On the use of Commercial Standards in Government IT Acquisitions

Date: July 31, 2024

Sponsor: Theresa Kinney, Deputy Director, NASA SEWP

Author: Jon Johnson, Strategic Advisor, NASA SEWP

Contributors: Alexander Marshall, Technical Strategist, NASA SEWP
Christopher Walker, Policy Analyst, NASA SEWP

About NASA SEWP

NASA SEWP is the first government-wide acquisition contract (GWAC), and the largest acquisition vehicle used by the entirety of the Federal Government. The program's involvement in international commercial standards spans over 20 years.

Table of Contents

Executive Summary

Government leverages commercial standards in Federal acquisitions now more than ever. It should… after all Congress and the Executive Branch and OMB required it of us. From the legislative definitions adopted in the 1970's[1], to the Clinton Administration of the 1990's[2], through to the Biden Administration[3]; commercial standards are encouraged, developed, and applied to industry and government. OMB Circular No. A-119[4] directed "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."[5] It continues, "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)."[6] The message should be clear – use commercial standards or give us a reason why you are not doing so.

NIST uses commercial standards to inform their publications. Sometimes they tie their recommendations directly to commercial standards. They did so directly in Appendix D of NIST SP 800-171 Rev.2 "Protecting Controlled Unclassified Information in Non-Federal Systems"[7] by providing a map of their recommendations and commercial controls found to meet Federal needs. Sometimes NIST just references a commercial standard, or key standards, as influence into their recommendations as they do in NIST SP 800-161 Rev.1 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations".[8]

Even if mentioned in reference, their position as to consider standards is clear and the reasons why should be self-evident. For example, in NIST 800-161Rev.1 NIST states "When possible and appropriate, acquirers should allow suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers the opportunity to reuse applicable existing data and documentation which 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*. *[Emphasis added]*".[9]

The use of commercial standards, however, is not something taught but rather something learned with experience. They appear in various procurements for a host of acquisitions dealing with people and products, as well as services and solutions. Contracting Officers and Program Offices often use standards for reference, to accept documentation as a functional baseline, as part of requirements definition, or as evidence of adhering to certain features called for in NIST recommendations. For government to "allow suppliers… the opportunity to reuse existing data

[1] https://www.law.cornell.edu/uscode/text/15/788
[2] https://www.nist.gov/standardsgov/national-technology-transfer-and-advancement-act-1995
[3] https://www.nist.gov/standardsgov/usg-nss
[4] https://obamawhitehouse.archives.gov/omb/circulars_a119
[5] Ibid.
[6] Ibid
[7] https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
[8] https://csrc.nist.gov/pubs/sp/800/161/r1/final
[9] Ibid. Page 12

and documentation"[10] used to secure their applicable commercial standard, it is helpful for Federal Agency personnel to gain an understanding of the standards themselves.

Gaining a nuanced level of understanding on the application of commercial standards is no easy task. We say so from experience. [11][12] What is the scope of the standard? What are the activities covered within the controls of that standard? What are the criteria used to validate or vet company practices in accordance with that commercial standard? How well the commercial standard controls map to what NIST recommends? These are the questions to address for an agency to determine acceptable and appropriate use of that commercial standard.

This whitepaper, however, is foundational way to understand what commercial standards are, and which are commonly applied to Federal ITC and AV related acquisitions.

'Who for' and 'Why'?

This whitepaper is for Federal personnel looking at the use of commercial standards in Federal procurement – Contracting offices, IT Program offices, CISO offices, or Policy offices.

This whitepaper serves as an introduction to a topic, something to consider as you engage in buying practices, to better understand the common language of best commercial practices, or and as a means to better understand where to go to find out more information on accepted commercial industry practices and approaches on a host of topics.

Scope

This white paper will answer the following three questions:

- What are commercial standards?
- Who makes them?
- Which ones are commonly used?

Introduction to Commercial Standards

The Definition of Commercial Standards

Legislative Branch Definition

"According to 15 U.S.C. § 788(f), Commercial Standards are:

[10] Ibid.

[11] https://www.sewp.nasa.gov/documents/OTTPS-NIST_CrossWalk_NASA_SEWP.pdf

[12] https://www.sewp.nasa.gov/documents/OTTPS-NIST_CrossWalk_NASA_SEWP_UPDATE.pdf

1) Specifications of materials.
2) Methods of testing.
3) Criteria for adequate performance or operation.
4) Model codes.
5) Classification of components.
6) Delineation of procedures or definition of terms.
7) Measurement of quantity or quality for evaluating or referring to materials, products, systems, services, or practices.
8) Similar rules, procedures, requirements, or standards.

…which are promulgated by any organization which is not a Federal entity.” [13]

Executive Branch Definition

Commercial Standards are common language for private sector practices. According to NIST, “Standards are essential to commerce, allowing technology to work seamlessly and business to operate smoothly. They provide industries and innovators with a common language which facilitates trade, simplifies transactions, and enables people to work together toward greater common goals which cut across disciplines and borders.”[14]

Industry Definition

According to Wikipedia, Commercial Standards are technical standards[15] organized by a standards organization[16] whose work is to create consensus between companies, stakeholders, and other interested parties which results in the development, coordination, release, and update of a specific technical standard. Standards are voluntary commitments; however, evidence of a company adhering to those commitments in practice can result in certification or accreditation (self-certified or 3rd party attested). Finally, International Standards Organizations engage in standards development which are considered for worldwide use and international acceptance.[17]

International Commercial Standards Organizations

There are a number of international standards organizations, however the three most prominent are considered to be the International Organization for Standardization (ISO)[18], the International Electrotechnical Commission (IEC)[19], and the International Telecommunication Union (ITU).[20]

[13] https://www.law.cornell.edu/uscode/text/15/788
[14] Ibid.
[15] https://en.wikipedia.org/wiki/Technical_standard
[16] https://en.wikipedia.org/wiki/Standards_organization
[17] https://en.wikipedia.org/wiki/International_standard
[18] https://www.iso.org/home.html
[19] https://www.iec.ch/homepage
[20] https://www.itu.int/en/Pages/default.aspx

These three organizations serve as governing bodies for the development, management, and approval of their respective international standards.

International Organization for Standardization (ISO)

"The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from more than 160 countries, one from each member country. ISO is a non-governmental organization established in 1947 and based in Geneva. Its mission is to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity."[21]

International commercial standards included in the ISO portfolio include:

- Quality Management Standards
- Environmental Management Standards
- Health and Safety Standards
- Energy Management Standards
- Food Safety Standards
- IT Security Standards[22]

*For more information on the International Organization for Standards, **click here**.*

[21] https://ansi.org/iso/us-representation-in-iso/introduction

[22] https://www.iso.org/standards.html

International Electrotechnical Commission (IEC)

"The IEC is one of the bodies recognized by the World Trade Organization (WTO) and entrusted by it for monitoring the national and regional organizations agreeing to use IEC International Standards as the basis for national or regional standards as part of the WTO Technical Barriers to Trade Agreement."[23]

International commercial standards in the IEC portfolio include the following sectors:

- Energy
- Sustainable Development Goals
- Climate Action
- Smart Manufacturing
- Healthcare
- Artificial Intelligence
- Transportation
- Cyber security
- Quantum Technology[24]

*For more information on the International Electrotechnical Commission, **click here**.*

International Telecommunications Union (ITU)

"ITU is the United Nations specialized agency for information and communication technologies (ICTs). The Organization is made up of a membership of 193 Member States and more than 1000 companies, universities and international and regional organizations. Headquartered in Geneva, Switzerland, and with regional offices on every continent, ITU is the oldest agency in the UN family – connecting the world since the dawn of the telegraph in 1865."

International commercial standards in the ITU portfolio include the following sectors:

- Power generation, transmission, and distribution
- Semiconductors and Fiber Optics
- Batteries and Solar Energy
- Nanotechnology

*For more information on the International Telecommunication Union, **click here**.*

[23] https://www.iec.ch/publications/international-standards

[24] https://www.iec.ch/where-we-make-difference

Other International Standards Organizations

The Open Group

"The Open Group is a global consortium that enables the achievement of business objectives through technology standards and open-source initiatives by fostering a culture of collaboration, inclusivity, and mutual respect among our diverse membership of more than 900 organizations. Our Membership includes customers, systems and solutions suppliers, tool vendors, integrators, academics, and consultants across multiple industries."[25]

The Open Group portfolio of standards include:

- Enterprise, Service Oriented, and IT Reference Architecture Standards
- Enterprise Management Standards
- Interoperable Applications and Embedded Systems Standards
- Open Group Trusted Technology Standards

*For more information on The Open Group, **click here**.*

Institute of Electrical and Electronic Engineers (IEEE)

"IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity… [and a] leading developer of international standards that underpin many of today's telecommunications, information technology, and power-generation products and services."[26]

The Open Group portfolio of standards include:

- Aerospace
- Electronic Communications
- Computer Technology
- Consumer Electronics
- Cyber Security
- Electrical Safety
- Nuclear Power
- Power and Energy
- Software and Systems
- Transportation
- Wired and Wireless Communications[27]

[25] https://www.opengroup.org/about-us

[26] https://www.ieee.org/about/at-a-glance.html#standards

[27] https://standards.ieee.org/standard/

*For more information on IEEE, **click here**.*

US-Based Standards Organizations

American National Standards Institute

"ANSI facilitates the development of American National Standards (ANS) by accrediting the procedures of standards developing organizations (SDOs) and approving their documents as American National Standards (ANS). [They are also] the sole U.S. representative to the International Organization for Standardization (ISO), [where they were a founding member, and] to the International Electrotechnical Commission (IEC)."[28]

*For more information on ANSI, **click here**. (*Purchasing from ANSI in USD to access ISO or IEC standards)*

Government and Commercial Standards

As mentioned in the introduction, government involvement and investment in the use of commercial standards is clear and widespread. On occasion, the US Government will support the creation of specific standards which address critical needs. For example, in 2010 the Department of Defense and NASA worked with The Open Group to develop The Open Technology Trusted Provider Standard (O-TTPS) to help address prominent threats for counterfeit and the malicious tainting when building and delivering COTS ICT products.[29] In section 888 of the 2016 NDAA Congress required that the DOD "shall conduct an assessment of the application of the Open Trusted Technology Provider Standard… to determine what aspects might be adopted by the Department of Defense and where additional development of the standard may be required."

NIST clearly has interest in standards development (*I mean come on people…. it's in their name!!!*). NIST closely monitors standards creation and account for them when creating their recommendations (which themselves become standards once included and adopted by Federal Agencies in requirements and responses to by their industry/contracting partners). The use of standards by NIST to help inform their recommendations became clear in our previous studies.[30][31]

[28] https://www.ansi.org/about/roles

[29] https://en.wikipedia.org/wiki/Open_Trusted_Technology_Provider_Standard

[30] https://www.sewp.nasa.gov/documents/OTTPS-NIST_CrossWalk_NASA_SEWP.pdf

[31] https://www.sewp.nasa.gov/documents/OTTPS-NIST_CrossWalk_NASA_SEWP_UPDATE.pdf

Lastly, Federal buyers use standards as a requirements indicator or as a means for companies to prove their capabilities. NASA SEWP[32], NITAAC[33], and the General Services Administration[34][35] all require contractors prove capabilities through commercial standards, as does the DOD[36].

Common Standards Required in Government Acquisitions

The following are commercial standards commonly found in Federal Government acquisitions. The description of each standard is directly from the standards website.

ISO 9001 – Quality Management

ISO

International Standard

ISO 9001:2015

Quality management systems — Requirements

Edition 5
2015-09

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:

1. **Context of the organization** – ISO 9001 requires organizations to determine the external and internal factors which affect their ability to achieve the intended results of their quality management system.
2. **Leadership** – The standard emphasizes the importance of leadership in implementing and maintaining a quality management system.
3. **Planning** – The quality management system must include measures designed to achieve an organization's quality objectives and continuously improve the system's effectiveness.
4. **Support** – ISO 9001 addresses issues such as resources, competence, awareness, communication and documented information.
5. **Operation** – The processes necessary to meet customer requirements and increase customer satisfaction must be planned, implemented and controlled.
6. **Performance evaluation** – The standard requires organizations to monitor, measure, analyze and evaluate the performance and effectiveness of their quality management system.
7. **Improvement** – ISO 9001 emphasizes the importance of continuously increasing the effectiveness of the quality management system based on the results of performance evaluation and other data sources.[37]

More information on the ISO 9000 Family, click **HERE**.
To purchase this standard, click **HERE**.

[32] https://www.sewp.nasa.gov/sewpvi/
[33] https://sam.gov/opp/97f5e6b5dd57497da0c67379462f8b1c/view
[34] https://sam.gov/opp/3ee6d8ff2d974744b3c0dc3325695b64/view
[35] https://sam.gov/opp/1a0fe6caac474a54aa63c047a960e99c/view
[36] https://www.dau.edu/acquipedia-article/capability-maturity-model-integration-cmmi
[37] https://www.iso.org/standard/62085.html#lifecycle

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. This standard can be used by:

International
Standard

ISO/IEC 20000-1:2018

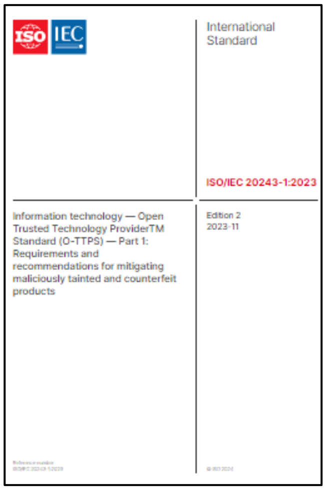
Information technology — Service management — Part 1: Service management system requirements

Edition 3
2018-09

1) A customer seeking services and requiring assurance regarding the quality of those services.
2) A customer requiring a consistent approach to the service lifecycle by all its service providers, including those in a supply chain.
3) An organization to demonstrate its capability for the planning, design, transition, delivery and improvement of services.
4) An organization to monitor, measure and review its SMS and the services.
5) An organization to improve the planning, design, transition, delivery and improvement of services through effective implementation and operation of an SMS.
6) An organization or other party performing conformity assessments against the requirements specified in this document.
7) A provider of training or advice in service management.[38]

*More information on the ISO/IEC 20000 Family, **click here**.*
*To purchase this standard, **click here**.*

ISO/IEC 20243 — Open Trusted Technology Provider Standard (O-TTPS)



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

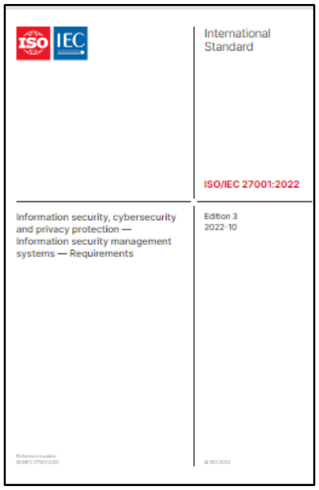
ISO/IEC 20243-1:2018 (O-TTPS) is a set of guidelines, requirements, and recommendations which address specific threats to the integrity of hardware and software COTS ICT products throughout the product life cycle. This release of the Standard addresses' threats related to maliciously tainted and counterfeit 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.[39]

*More information on the ISO/IEC 20243, **click here**.*
*To purchase this standard, **click here**.*

[38] https://www.iso.org/standard/70636.html
[39] https://www.iso.org/standard/86338.html

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


International Standard

ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Edition 3
2022-10

Reference number
ISO/IEC 27001:2022

© ISO 2022

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.[40]

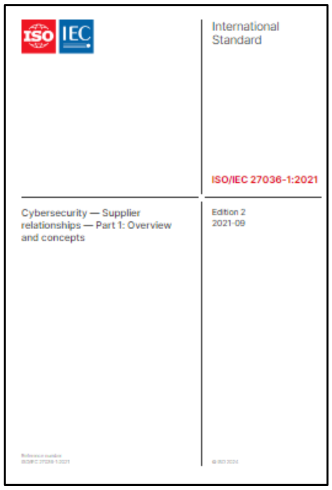
Implementing the information security framework specified in the ISO/IEC 27001 standard helps:

- Reduce vulnerability to the growing threat of **cyber-attacks**.
- Respond to **evolving security risks**.
- Ensure that assets such as financial statements, intellectual property, employee data and information entrusted by third parties remain **undamaged, confidential, and available** as needed.
- Provide a **centrally managed framework** which secures all information in one place.
- Prepare **people, processes and technology** throughout your organization to face technology-based risks and other threats.
- Secure **information in all forms**, including paper-based, cloud-based and digital data.
- **Save money** by increasing efficiency and reducing expenses for ineffective defense technology.[41]

*More information on the ISO/IEC 27000 Family, **click here**.*
*To purchase this standard, **click here**.*

[40] https://webstore.ansi.org/standards/iso/isoiec270012022
[41] https://www.iso.org/standard/27001

ISO/IEC 27036 — Cybersecurity — Supplier Relationships



International
Standard

ISO/IEC 27036-1:2021

Cybersecurity — Supplier relationships — Part 1: Overview and concepts

Edition 2
2021-09

ISO/IEC 27036[42] is also part of the ISO/IEC 27000 Family of information security standards.

This standard 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.[43]

Companies who meet this standard has, as an organization, internally implemented a number of foundational processes including business management, risk management, operational and human resources management, and information security. [44]

*To purchase this standard, **click here**.*

Other Approaches

The Federal Government has invested in security models which require industry prove that their practices conform to these models and achieve a resulting certification – not quite commercial standards, but not terribly different from them.

CMMI Institute & Capability Maturity Model Integration (CMMI)

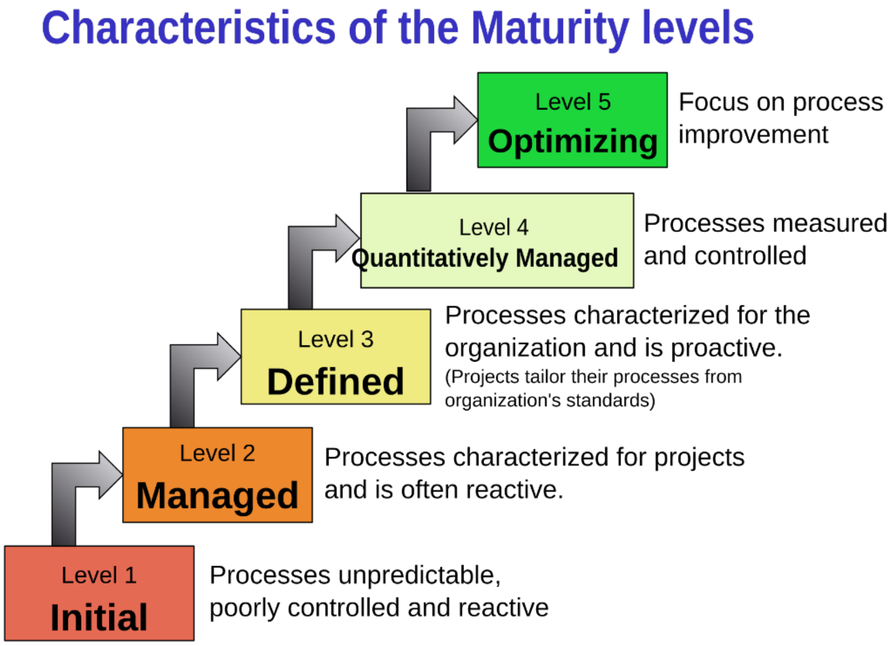
A model, not a standard. The Federal Government, particularly the Department of Defense, invested in creating a security model which require industry prove mature software development practices and achieve a scored assessment proving out the maturity level of a company's practices – not quite commercial standards, but not terribly different from them. CMMI assessments are required for software development contracts in the DOD, NASA, and throughout the Federal Government.

The CMMI Institute[45] originated with Carnegie Mellon University as they worked with the Department of Defense, industry, and academe to create the Capability Maturity Model Integration (CMMI) appraisal program[46]. The Information Systems Audit and Control Association

[42] https://www.iso.org/standard/82905.html
[43] https://webstore.ansi.org/standards/iso/isoiec270362022
[44] Ibid.
[45] https://cmmiinstitute.com/
[46] https://cmmiinstitute.com/cmmi/intro

(ISACA)[47], and International IT Governance Association, now holds the responsibility of owning and managing the CMMI model and its' appraisal and certification process.

Capability Maturity Model Integration (CMMI) is a process level improvement training and appraisal program and required by many of the governments' software development contracts. It defines five maturity levels (1 to 5) for processes – Initial, Managed, Defined, Quantitatively Managed, and Optimizing.[48] 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.[49]


Characteristics of the Maturity levels
Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive.
(Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive.
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

50

*To purchase access to CMMI Content, **click here**.*

*To learn more about the CMMI Appraisal Process, **click here**.*

*For more information on the CMMI Institute, **click here**.*

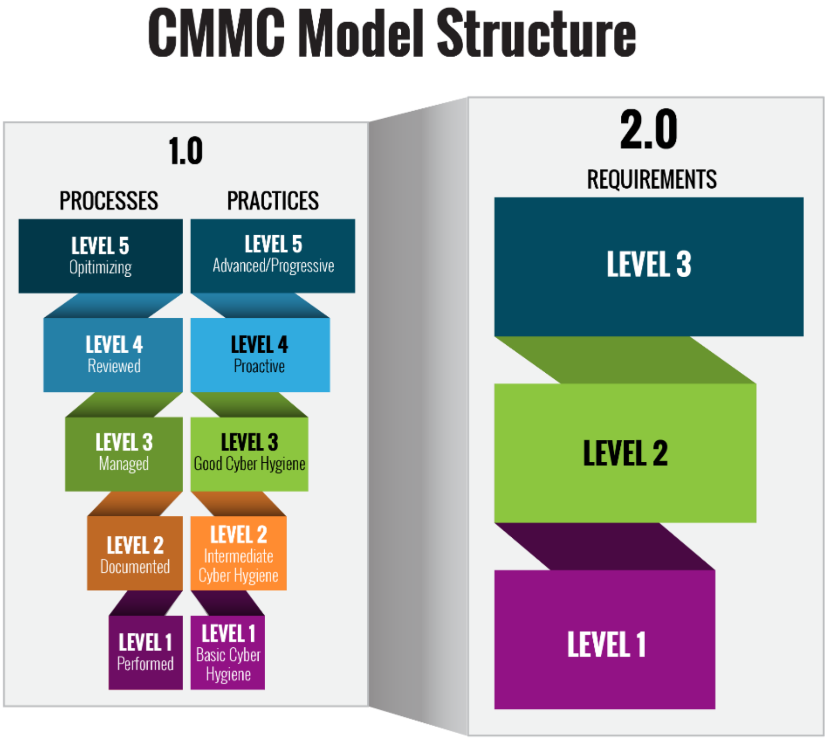
*For more information on ISACA, **click here**.*

[47] https://www.isaca.org/
[48] https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration
[49] https://cmmiinstitute.com/learning/appraisals
[50] Sally Godfrey (2008) [software.gsfc.nasa.gov/docs/What%20is%20CMMI.ppt What is CMMI?]. NASA presentation. Accessed 8 December 2008. - https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration#/media/File:Characteristics_of_Capability_Maturity_Model.svg

Cybersecurity Maturity Model Certification & The Cyber AB

An emergent program closely modeled on the CMMI is the Cybersecurity Maturity Model Certification (CMMC),[51] another Department of Defense initiated program developed with Carnegie Mellon University. CMMC "is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) which is shared with contractors and subcontractors of the Department through acquisition programs."[52]

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* [emphasis added], will be based on a subset of NIST SP 800-172 requirements."[53]



[54]

The mechanism for an "organization seeking [CMMC] certification"[55] is through the Cyber AB.[56] "The Cyber AB is the official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) Ecosystem and the sole authorized non-governmental partner of the U.S. Department

[51] https://dodcio.defense.gov/CMMC/Model/

[52] Ibid.

[53] https://dodcio.defense.gov/CMMC/Model/ - Frequently Asked Questions

[54] https://dodcio.defense.gov/Portals/0/Images/CMMC/cmmc2-levels-stv2.png

[55] https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles/DIB-Companies-OSCs

[56] https://cyberab.org/

of Defense in implementing and overseeing the CMMC conformance regime. The primary mission of The Cyber AB is to authorize and accredit the CMMC Third-Party Assessment Organizations (C3PAOs) which conduct CMMC Assessments of companies within the Defense Industrial Base (DIB)."[57]

This program is emergent as it is currently in Federal Acquisition Regulation rules making process and under comment collection and review. The Expert Level 3 is under development; therefore, current certifications are only to Level 2.

For more information on the DOD's CMMC Program, click here.
For more information on the Cyber AB, click here.

Conclusions, Considerations, and Challenges

The Federal Government has invested in the creation, use, and adoption of commercial standards for more than a century.[58] The Federal Government actively use commercial standards as a foundation for issuing guidance, or in their requirements when procuring Information and Communication Technology solutions to fulfill their mission needs. It is important to know about these standards, understand where they come from, what is required of companies to prove out practices which meet standards, and the scope of their assessments.

The NASA SEWP program often sits at the intersection of government and industry. We are the voice *of government to industry* when communicating with our contract holders and provider base. We are just as often the voice *of industry to government*; understanding the investment companies make; understanding the scope, limits, and promise of technology from private sector leaders; understanding the result prospects and impacts on industry concerning policy initiatives; and articulating and communicating the 2nd and 3rd order effect which often goes unspoken within the government community.

With this later role in mind, we offer a consideration, or an ask, for those involved in IT acquisitions and IT acquisition policy; government should seek ways to reduce the burden place onto industry by recognizing reciprocity of commercial standards in lieu of required documentation. The inter-relations between commercial standards, NIST recommendations, and the certification programs is clear. What is less clear is how these different pieces fit together.

Which is ***THE*** main challenge…isn't it? Standards are updated regularly, and often material is built around the standards to help with education and adoption. NIST Special Publications (SP) are updated just as often, if not more, and the Special Publications associated with IT inter-relate. A change in a foundational SP 800 series trickles through other parts. Further, accreditation bodies evolve in how they consider and evaluate a company's evidence of capabilities. It is difficult to create a static approach to variable conditions.

[57] https://cyberab.org/About-Us/Overview
[58] https://www.standardsportal.org/usa_en/standards_system.aspx

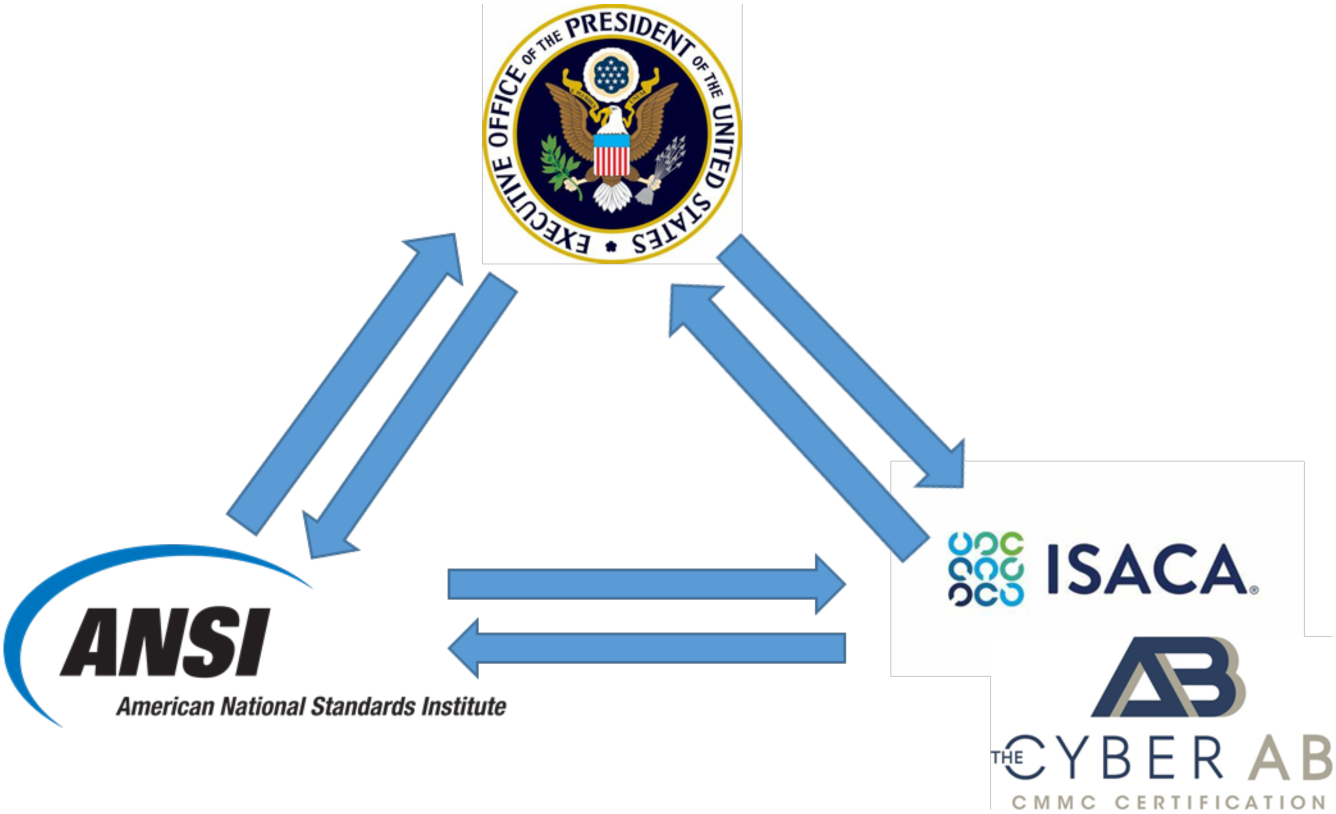
Overcoming this challenge would require at least three things:

1) Commercial Standards bodies consider how their standards meet the requirements of industry in accordance with NIST guidance and recommendations.

2) NIST, working jointly with Standards Bodies, clarify the connections between what Commercial Standards and NIST require of industry controls.

3) Accreditation Bodies, working with Commercial Standards bodies and NIST, can then accept the ISO Standard (with the appropriate verification) in lieu of requests for additional information and only ask for discrete evidence of those controls not covered by the standard.

Note: *This can also happen in reverse where Federal accreditation is applicable to ISO standards, thereby putting a company in position to apply those investments into the commercial marketplace. For example, commercial practices evaluated as part of CMMI can be applied to ISO 9001 (Quality Management) and ISO/IEC/IEEE 12207 (Software Process Lifecycle).*


EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
ANSI
American National Standards Institute
ISACA
THE CYBER AB
CMMC CERTIFICATION

Author’s Note

Thank you to our many colleagues in government and industry who contributed to this topic with a particular emphasis on the Cybersecurity Supply Chain Risk Management (C-SCRM) 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. Finally thank you to the NASA SEWP Program for continuing to be a brain and a bridge which connects the Federal Government and industry.