A STANDARDS-BASED APPROACH TO ADVANCING INFORMATION SECURITY

CONSIDERATIONS FOR GOVERNMENT AND INDUSTRY

Jon Johnson, Strategic Advisor
NASA SEWP Program

THE NASA SEWP PROGRAM

- United States Government Contract Vehicle for ICT (Information & Communication Technology) and Audio/Visual (AV) Solutions
  - Utilized by every Federal Agency
  - 140+ Contract Holders – primarily Resellers/Integrators
  - Over 9700 Manufacturers and Service Providers
  - Annual Obligated Value Over $12.5B
  - Accounts for about 16% of the government's IT budgetary spend.*

(*78B in FY23 according to Gov)

THE NASA SEWP PROGRAM

The NASA SEWP Program Management Office performs many roles in support of Government Acquisition:

- Oversee and monitor Contract Holders and Industry Relations
- Mediate actions between Government and Industry
- Support, track, and verify supply chain relationships
- Expedite addition of current and emerging technology based on customer requirements
- Inform the Government customer on overall Contract processes and specific policy-related aspects of their acquisition

NASA SEWP AND SUPPLY-CHAIN RISK MANAGEMENT

The SEWP Program has participated in The Open Group throughout their 25-year history with particular focus on:

- Long time participation in Security Forum
- Open Trusted Technology Forum
- Recent activity in IT4IT and Architecture Forums

Participation has provided a better Program Understanding:

- Global range of IT-related Issues
- Industry concerns, solutions, conflicts and differences (Governments tend to consider Industry to be a monolithic entity)
- Supply Chain issues and some paths forward

2021 STANDARDS CROSS-WALK

2021 STANDARDS CROSS-WALK

OMB Circular NO.A-119 states “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.

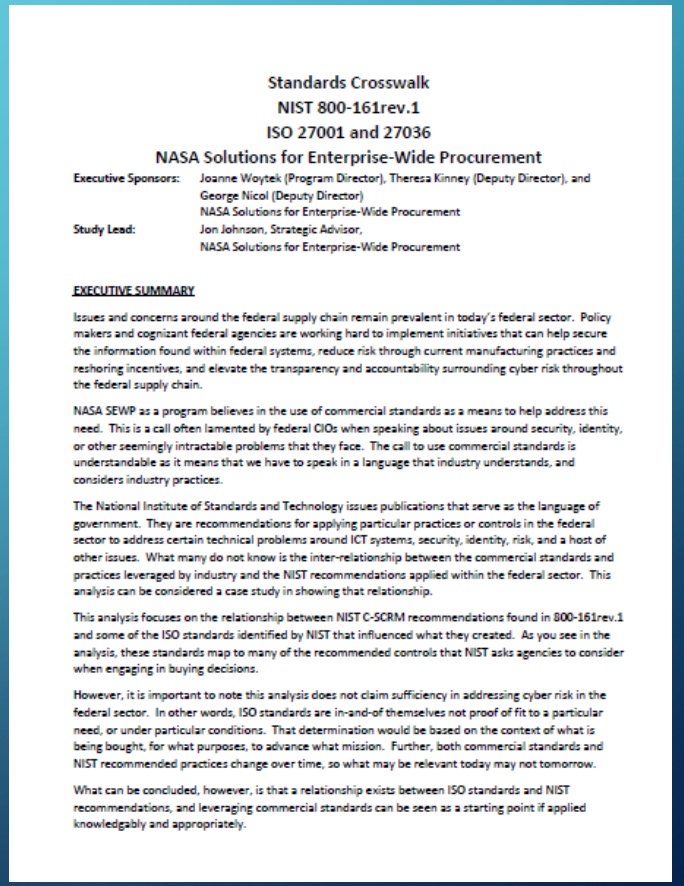
Does ISO 20243 satisfy specific elements required or recommended through NIST SP 800-161? If so, what are they exactly? Can the ISO 20243 standard be used as a tool for agencies to assist in SCRM related processes? If so, how?

2021 STANDARDS CROSS-WALK

- The ISO 20243 SCRM Standards map to between 75-89% of the supplier risk controls recommended in NIST IR 7622;
- The ISO 20243 SCRM Standards fully addresses 5 of the 12 Supply Chain Management Control Enhancements found in the existing NIST 800-161;
- The ISO 20243 SCRM Standard satisfies 9 of the 12 Supply Chain Management Control Enhancements and compliments 2 of the remaining 3 controls found in the existing NIST 800-161;
- There is only one Supply Chain Management Control Enhancement Control in NIST 800-161 that ISO 20243 SCRM cannot satisfy and does not address.

At the time of release we knew NIST was developing 161rev.1. We also knew that we wanted to revisit the other foundational ISO standards that NIST considered.

2023 STANDARDS CROSS-WALK



Standards Crosswalk
NIST 800-161rev.1
ISO 27001 and 27036
NASA Solutions for Enterprise-Wide Procurement

Executive Sponsors: Joanne Woytek (Program Director), Theresa Kinney (Deputy Director), and George Nicol (Deputy Director)
NASA Solutions for Enterprise-Wide Procurement

Study Lead: Jon Johnson, Strategic Advisor,
NASA Solutions for Enterprise-Wide Procurement

EXECUTIVE SUMMARY

Issues and concerns around the federal supply chain remain prevalent in today's federal sector. Policy makers and cognizant federal agencies are working hard to implement initiatives that can help secure the information found within federal systems, reduce risk through current manufacturing practices and reshoring incentives, and elevate the transparency and accountability surrounding cyber risk throughout the federal supply chain.

NASA SEWP as a program believes in the use of commercial standards as a means to help address this need. This is a call often lamented by federal CIOs when speaking about issues around security, identity, or other seemingly intractable problems that they face. The call to use commercial standards is understandable as it means that we have to speak in a language that industry understands, and considers industry practices.

The National Institute of Standards and Technology issues publications that serve as the language of government. They are recommendations for applying particular practices or controls in the federal sector to address certain technical problems around ICT systems, security, identity, risk, and a host of other issues. What many do not know is the inter-relationship between the commercial standards and practices leveraged by industry and the NIST recommendations applied within the federal sector. This analysis can be considered a case study in showing that relationship.

This analysis focuses on the relationship between NIST C-SCRM recommendations found in 800-161rev.1 and some of the ISO standards identified by NIST that influenced what they created. As you see in the analysis, these standards map to many of the recommended controls that NIST asks agencies to consider when engaging in buying decisions.

However, it is important to note this analysis does not claim sufficiency in addressing cyber risk in the federal sector. In other words, ISO standards are in-and-of themselves not proof of fit to a particular need, or under particular conditions. That determination would be based on the context of what is being bought, for what purposes, to advance what mission. Further, both commercial standards and NIST recommended practices change over time, so what may be relevant today may not tomorrow.

What can be concluded, however, is that a relationship exists between ISO standards and NIST recommendations, and leveraging commercial standards can be seen as a starting point if applied knowledgably and appropriately.

2023 STANDARDS CROSS-WALK

The **purpose** of this study is to see how well specific commercial standards map to NIST recommended controls found in NIST SO 800-161rev.1.

The **goal** of this effort is to continue bringing awareness to the inter-relation between NIST recommended controls and standards and practices accepted by the commercial sector.

One **intended outcome**, should a standard prove to meet a majority of recommended controls, would be to *identify a means for government and industry to prove competency of practices and show how they may account for identified provider actions recommended by NIST*.

To what extent are ISO 27001 and ISO 27036 standards applicable to NIST 880-161rev.1? How do the standards relate to one another? Can they be mapped to determine if they complement or contradict one another? To what extent can they be used by agency buyers to help fulfill their obligations associated with NIST 161rev.1?

2023 STANDARDS CROSS-WALK

NIST 161rev.1 contains 182 controls organized accordingly:

Family >
Control Number >
Control Title >
Control Description & Requirements >
Responsible Party/Tier

The Responsible Party/Tier indicated the responsible party and is broken up accordingly:

Level	Name	Role	Generic Stakeholder
1	Enterprise	Executive Leadership	CEO, CIO, COO, CFO, CISO, Chief Technology Officer (CTO), Chief Acquisition Officer (CAO), Chief Privacy Officer (CPO), CRO, etc.
2	Mission and Business Process	Business Management	Program management [PM], project managers, integrated project team (IPT) members, research and development (R&D), engineering (SDLC oversight), acquisition and supplier relationship management/cost accounting, and other management related to reliability, safety, security, quality, the C-SCRM PMO, etc.
3	Operational	System Management	Architects, developers, system owners, QA/QC, testing, contracting personnel, C-SCRM PMO staff, control engineer and/or control system operator, etc.

Each control was identified to see if there was a corresponding action required by the supply base. Out of the 182 controls, 66 were identified (approximately 36% or just over 1/3) as a recommendation with identified accountability, responsibility, or action on behalf of the private sector supplier base.

2023 STANDARDS CROSS-WALK

ISO/IEC 27001:2022 “Information security, cybersecurity and privacy protection — Information security controls” outlined a control structure for Organizational Controls (Section 5), People Controls (Section 6), Physical Controls (Section 7), and Technological Controls (Sections 8).

- A Control Title – A short name identifying the control;
- An Attribute Table – A table that shows the value of each attribute for the given control;
- Control – What the control is;
- Purpose – Why the control should be implemented;
- Guidance – How the control should be implemented;
- Other information – Explanatory text or referenced to other related documents

2023 STANDARDS CROSS-WALK

ISO 27036 advances cybersecurity considerations into the supplier relationships and is tightly couple with requirements found in ISO 27002 for Information Security Management, effectively pressing for the communication of standards and accountability down into their supplier relationships.

Annex B “Correspondence between ISO/IEC 27002 controls and this document.” This appendix provides a table that maps the controls identified to 49 control groups found in ISO 27002, and proved to be particularly useful when conducting the analysis.

Annex C “Objectives from Clauses 6 and 7.” laid out 23 respective controls found in applied to the Acquirer (Buyer) and the Supplier (Seller) side of the contractual equation.

2023 STANDARDS CROSS-WALK

By breaking down each individual standard document into their component controls or activities, the process of cross referencing drew out the overlap between the standards and controls in a manageable way.

The recommended NIST controls for a C-SCRM baseline, applicable to the federal supplier base were identified, Information, including the number and description, for each control was captured in a spreadsheet and organized by NIST Control Families.

Then each individual ISO standard was reviewed to see if an identified standard or description appeared to satisfy the associated NIST Control.

ISO/IEC 27036 – Information Security for Supplier Relationships

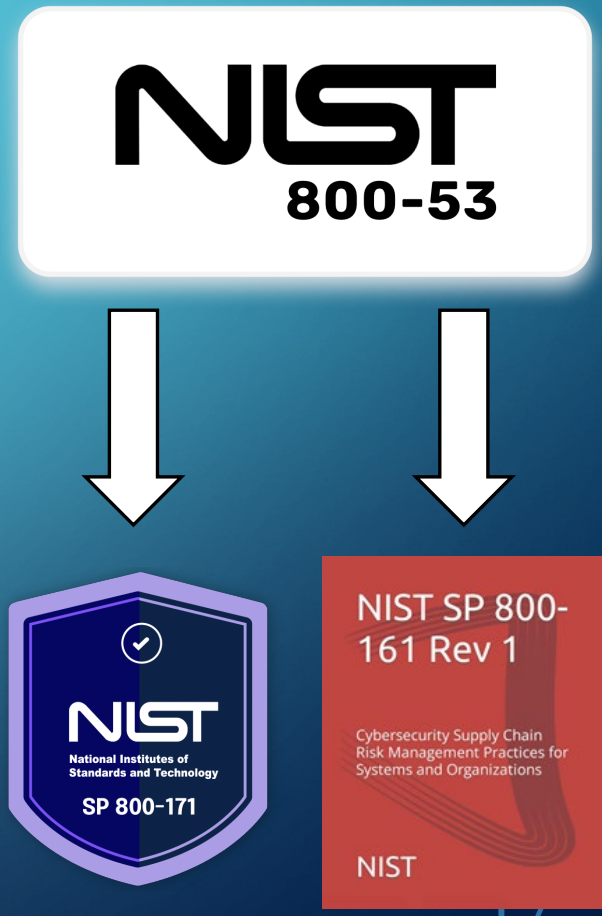
2023 STANDARDS CROSS-WALK

The study had to impose quality control over interpretations. Fortunately, prior to conducting the individual mapping of NIST 800-161rev.1, NIST 800-171rev.2 was consulted.

Appendix D of NIST 800-171rev.2 provided a mapping of the supply-chain security controls found in ISO 27001 to the relevant security controls found in NIST 800-53rev.5 “Security and Privacy Controls for Information Systems and Organizations”.

NIST 800-53 serves as the anchor for the controls used by other NIST publications, including NIST 800-171rev.2 and NIST 800-161rev.1.

Therefore, any control number of ISO 27001 that had been mapped by NIST 800-171 as being complimentary to that effort could be used to provide a quality review of the study’s mapping.



2023 STANDARDS CROSS-WALK

Each identified C-SCRM baseline or supplier control and their associated control number was captured on a spreadsheet. Those controls that came pre-mapped as indicated in NIST 800-171rev.2 were identified. The remaining controls were then compared to the ISO standard controls to see if there was a mapping. The general analysis found:

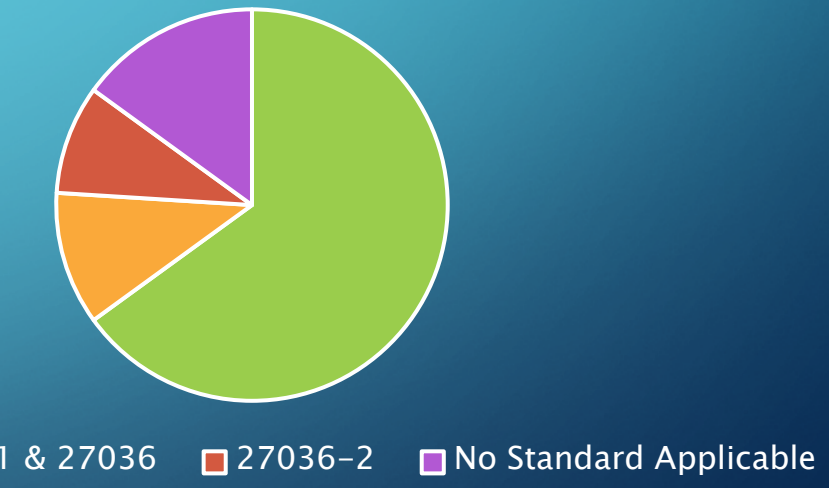
- Some of the NIST controls were met by considering a basket of ISO standard controls;
- Some of the NIST controls were accounted for by combining the Information Management requirements of 27001 with the Supplier Management activities found in 27236-2 ;
- Still other NIST controls were only capable of being met by mapping exclusively to ISO 27236-2

2023 STANDARDS CROSS-WALK

The results indicated a clear mapping of control sets between those recommended for suppliers in NIST 800-161rev.1 and ISO 27001 and 27036-2.

- 65% of the individual vendor controls can be accounted for through ISO 27001 alone;
- 9% of the vendor controls can be accounted for by ISO 27036 alone;
- 11% of the individual vendor controls can only be accounted for by combining ISO 27001 and 27036;
- 15% of the individual vendor controls cannot be addressed by either ISO standard.

Applicable to NIST 800-161rev.1



85% of the recommendations stated by NIST can be satisfied by a company holding ISO 27001 and 27036.

CROSSWALK LIMITATIONS

NIST requirements and ISO standards change.

Agency missions' vary.

Interpretations were required to draw conclusions.

We don't cover the role of attestation.

CROSSWALK IMPLICATIONS

- There is utility of leveraging ISO standards as a means to help secure the government's security posture.
- Agencies should know what commercial standards cover and make use of them as a basis for security as they see fit.
- ISO standards bodies should put forth the efforts to detail how their standards match NIST recommendations.
- Reciprocity will always be an issue.

QUESTIONS

?