ICT SCRM builds on other disciplines and requires a certain level of maturity to succeed

Tools and Techniques

- Common Criteria
- OMG KDM BPMN, RIF, XMI, RDF
- OWASP Top 10
- SANS TOP 25
- Secure Content Automation Protocol (SCAP)
- Secure Coding Checklists
- Encryption
- Security Engineering and Design techniques
- NASPO and other Anti - Counterfeiting techniques
- Software Asset Tagging

ICT SCRM and other Context-Specific Requirements

- ISO/IEC 27036 Part 3 – ICT SCRM; Part 4 – Cloud;
- NIST SP 800-161
- **SAE AS5553** Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
- **SAE AS6462A - AS5553A** Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria

ICT SCRM General Requirements

- ISO/IEC: 27036 Parts 1 – Overview Part 2: Requirements
- ISO/IEC 20243:2015- .Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.0

Essential Security and Foundational Practices

- **Management Systems**: ISO 9001 - Quality, ISO 27001 – Information Security, ISO 20000 – IT Service Management, ISO 28000 – Supply Chain Resiliency
- **Security Controls**: ISO/IEC 27002, NIST 800-53
- **Lifecycle Processes**: ISO/IEEE 15288 - Systems, ISO/IEEE 12207 - Software
- **Risk Management:** ISO 31000 - overall, ISO/IEC 27005 - security, and ISO/IEC 16085 - systems
- **Industry Best Practices:** CMMI, Assurance Process Reference Model, Resiliency Management Model (RMM), COBIT, ITIL, PMBOK

Processes and Practices

- **ISO/IEC 15026 – System & Software Assurance**
- **ISO/IEC 27034 – Application Security**
- **ISO/ IEC 27035 Information security incident management**
- **ISO 3011 Vulnerability handling processes**
- **ISO/IEC 29147:2014 Vulnerability disclosure**
- **Industry: Microsoft Secure Development Lifecycle (SDL)**
- **SAFECode**
- **OWASP**
- **BSIMM**

August 10, 2015

Comment Template for NISTIR 8074 Volume 1, Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (Draft)

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1		Major	1:6	Standards are often ignored by leadership. The first part of the document should include why standards are important and why cybersecurity standards are important. We want a level playing field basically—a set of standardized expectations, language, etc when we are working with international partners who are comprised of many other levels of international participation. Code and parts that come from all over the world, are then assembled and shipped to anywhere. International discussion and agreement gives us insight into other nation's interests, etc. With the cooperation and understanding of international partners we can ensure the safety and legal rights of US interests and businesses.	Add an introduction that 1) speaks to the economic importance of standards (entry into global markets and the use of standards in international trade agreements (i.e. WTO) 2) introduces the concept that cybersecurity standards build on practices that are expected from other standards. 3) Points to additional details in the supplemental information.
2		Major	2;46	There is a misperception that US positions are generated by US citizens. This is not always the case. Foreign companies in the US can be members and foreign nationals may represent the company and contribute to the US position	Add that the market forces may include foreign influence to the US positions and may not always represent the best interest of the US.
3		Major	1-2	There is a lot of content and details. The key points get lost. Either add as a BLUF summary in the intro or add an executive summary that speaks to the economic importance, dependence on foundational standards not otherwise considered "cybersecurity", and the key elements to success.	add key elements to success 1) Ensure the expectations met and not met by a standard are understood by the decision makers 2) Ensure input from diverse organizational stakeholders that understand the business/mission needs, technical experts, and standards development experts. 3) US standards priorities should support domestic industrial and innovation policy 4) US standards efforts should be driven by the solution needs and not always the issue being solved (i.e. cyber challenges in voting technology, voting is not done in many other countries) 5) To the extent possible participation should be streamlined to minimize the cost of government and private sector involvement 6) Understanding and capitalizing on the interrelationship among standards (i.e. quality, engineering, asset management, configuration management, manufacturing, etc) 7) Building and maintaining the relationships and liaisons necessary to influence SDOs. 8) The development of core standards for a technical area, the subsequent tailoring to specific implementations will ensure a reference for new technologies and a baseline of knowledge across a multiple applications (i.e. cloud, mobile, health IT, etc)

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
					9) Incorporation of standards in agency policies 10) The number of cybersecurity standards projects is substantial; therefore an engagement model is required to ensure that the U.S. government is able to dynamically engage at the right level when necessary.
4		Major	3;107	This content from the supplemental information is valuable and should be included in the Report.	Participants must attend the meetings regularly over a period of one or more years and have established relationships with the other participants to facilitate necessary progress in moving the agenda forward and ensuring that the draft standards are technically sound and meet USG needs. It is important to understand and take advantage of the fact that negotiations occur before, after, during and in between the formal meeting sessions. Effective leadership in SDOs promotes timely development of technically sound standards. It is in the best interest of Federal agencies to support qualified Federal representatives (including contracted technical experts) in SDO leadership positions. Candidates for such leadership positions should be both technically knowledgeable and thoroughly familiar with the SDO's development processes and policies. Key SDO leadership positions include chairing or convening groups, providing the administrative/secretariat functions for groups, and serving as the project editor for a specific standards development project. Office of Management and Budget (OMB) Circular A-119 [Section 15. b. (3)] emphasizes the need for interagency coordination and cooperation in voluntary standards development: "Ensuring, when two or more agencies participate in a given voluntary consensus standards activity, that they coordinate their views on matters of paramount importance so as to present, whenever feasible, a single, unified position and, where not feasible, a mutual recognition of differences." The USG also needs to effectively engage with U.S. stakeholders. There are several methods agencies can use to engage and coordinate with stakeholders. Agencies may choose to establish external advisory committees per the Federal Advisory Committee Act (FACA), seek input using Federal Register Notice solicitations, use specific statutory or

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
					regulatory authority to create a forum for obtaining input, or use some other method that provides all potential stakeholders an equal opportunity to provide input and share their perspectives.

August 10, 2015

Comment Template for NISTIR 8074 Volume 2, Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (Draft)

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1		Major	4; 167	How were these areas determined? Information Sharing (i.e. of threat information) and asset management are also important.	Please explain the rational for determining these areas and when/how they might evolve.
2		Major	9; table 2	Industry guidance is often input into standards.	Add a maturity level "Guidance Available" with Definition industry guidance is available indicating there may be sufficient understanding and content to codify the information in a standard"
3		Major	17	Industry views SCRM as a multi discipline area and there are standards that currently exist.	Add • **SO/ IEC 27036-1:2014** Information technology -- Security techniques -- Information security for supplier relationships (Part 1: Overview and concepts)[1] • **ISO/ IEC 27036-2:2014** Information technology -- Security techniques -- Information security for supplier relationships (Part 2: Common requirements)[2] • **ISO/ IEC 27036-3: 2013** Information technology -- Security techniques -- Information security for supplier relationships (Part 3: Guidelines for ICT supply chain security)[3] • **Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.0 -** Mitigating Maliciously Tainted and Counterfeit Products (also approved as an ISO/IEC International Standard (ISO/IEC 20243:2015). • **SAE AS5553** Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition[4] • **SAE AS6462A - AS5553A** Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria[5] • **ISO/ IEC 27035** Information technology -- Security techniques -- Information security incident management[6]

[1] http://www.iso.org/iso/catalogue_detail.htm?csnumber=59648
[2] http://www.iso.org/iso/catalogue_detail.htm?csnumber=59648
[3] http://www.iso.org/iso/catalogue_detail.htm?csnumber=59688
[4] http://standards.sae.org/as5553/
[5] http://standards.sae.org/as6462a/
[6] http://www.iso.org/iso/catalogue_detail?csnumber=44379

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
					• **ISO 3011** Information technology -- Security techniques -- Vulnerability handling processes[7] • **ISO/IEC 29147:2014** Information technology -- Security techniques -- Vulnerability disclosure[8]
4		Major	17	Industry views Software Assurance as a multi disciple area and there are standards that currently exist.	Add • **ISO/IEC TR 24772:2010** Information technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use[9] • **ISO/ IEC 27034-1: 2011** Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts[10] • **ISO/IEC FDIS 27034-2** Application security (Part 2: Organization normative framework) • **Under development ISO/IEC TR 19249** — Information technology — Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications. • **Under development ISO/IEC TR 24772 Edition 3** — Information technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use • **Under development ISO/IEC 17960** Source Code Signing • **Under development CISQ** Security measure is in process through OMG
5		Major	17	Industry views System Security Engineering as a multi disciple area and there are standards that currently exist.	Remove ISO/IEC 21827 as it is out dated and not adopted Add • **ISO/IEC 15026-2** Systems and software engineering -- Systems and software assurance (Part 2: Assurance Case)[11]

[7] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231
[8] http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170
[9] http://www.iso.org/iso/catalogue_detail.htm?csnumber=41542
[10] http://www.iso.org/iso/catalogue_detail.htm?csnumber=44378
[11] http://www.iso.org/iso/catalogue_detail.htm?csnumber=52926

#	SOURCE	TYPE i.e., Editorial Minor Major	PAGE; LINE # etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
					• **ISO/IEC 15026-4** Systems and software engineering -- Systems and software assurance (Part 4: Assurance in the life cycle)[12] • **NDIA SA Guide Book/NATO AEP-67** Engineering for System Assurance in NATO Programs

[12] http://www.iso.org/iso/catalogue_detail.htm?csnumber=59927