

**Comment Template for Draft NIST Interagency Report (NISTIR) 8200 -- Status of International Cybersecurity Standardization for the Internet of Things (IoT)**

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	ANAB	Major	Section 6.5	<p>Reference to ISO/IEC 27001, the certification standard for ISMS, is missing from the text.</p> <p>Organization should be encouraged to use IAF recognized accredited certification to ISO/IEC 27001. Accreditation bodies (AB) that are not signatory to the IAF or unaccredited certification bodies (CBs) or uncertified organizations may not operate according the specified requirements. These ABs and CBs may offer services without oversight or without any real understanding of an organization's processes. Such a certificate is of questionable value for the certified organization and its customers.</p> <p><b>Certification</b> – the provision by an independent body of written assurance (a certificate) that system meets specific requirements.</p> <p><b>Accreditation</b> is the process of ensuring that an organization has the necessary technical competence to perform a specific task, and has met and continues to meet a specific set of operational requirements.</p> <p>An accreditation body (AB) uses internationally established techniques and procedures to assess conformity assessment bodies (CABs) against recognized standards to ensure their impartiality, competence, and ability to produce consistently reliable, technically sound and impartial results.</p> <p>The international accreditation forum (IAF) provides oversight over ABs to ensure ABs are competent to provide accreditation services in a specific field.</p>	<p>ISO/IEC 27001 <i>Information technology - Security techniques - Information security management systems – Requirements</i> provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS).</p> <p>To ensure credibility and recognition of ISO/IEC 27001 certificates by various stakeholders globally, certification should be provided by a Certification Body accredited to the requirements of ISO/IEC 17021-1 for the scope of ISMS by an IAF MLA signatory Accreditation Body.</p>

**Comment Template for Draft NIST Interagency Report (NISTIR) 8200 -- Status of International Cybersecurity Standardization for the Internet of Things (IoT)**

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
2	ANAB	Major	Section 6.10	Reference to ISO/IEC 28000, the certification standard for SCMS, is missing from the text.  Same as above.	ISO 28000 <i>Specification for security management systems for the supply chain</i> , specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain.  To ensure credibility and recognition of ISO/IEC 28000 certificates by stakeholders globally, certification should be provided by a Certification Body accredited to the requirements of ISO/IEC 17021-1 for the scope of SCMS by an IAF MLA signatory Accreditation Body.
3	ANAB	Major	Section 8.5	Same as for section 6.5	Include reference to ISO/IEC 27001.

**Comment Template for Draft NIST Interagency Report (NISTIR) 8200 -- Status of International Cybersecurity Standardization for the Internet of Things (IoT)**

<b>COMMENT #</b>	<b>SOURCE</b>	<b>TYPE</b> i.e., Editorial Minor Major	<b>LINE #</b> <b>PAGE</b> etc.	<b>RATIONALE for CHANGE</b>	<b>PROPOSED CHANGE</b> (specific replacement text, figure, etc. is required)