February 12, 2018

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	Andrew Ginter, Waterfall Security Solutions	Major	Line 280-281	IoT safety needs to be first and foremost in your analysis. Consider simple examples: a worm exploits zero-days in network-connected stovetops, turning all of the burners to maximum at 2 AM Christmas day, for all stove-tops whose IP addresses identify them as being in the continental USA. Some home-owners left combustibles standing on what they thought was a turned-off stove. 1000 homes burn to the ground. 100 people die. A terror group takes responsibility. Or – a nation-state actor compromises the software update website for online-updateable automobiles, pushing out a new version of firmware that causes all of that vendor's supported models to accelerate to the maximum and veer hard left at 5:30 PM ET on a Wednesday, again for all autos with IP addresses in the USA. Carnage ensues on America's roadways during eastern and central rush hours. The president declares a national state of emergency. These are serious threats to consumer safety and to a degree the economy. Eg: repeat the automobile scenario with transport trucks and the economic impacts will be significant. IoT devices physically able to monitor the physical world are harmless – let the data-centric-security people worry about privacy issues. IoT devices that are able to control the physical world more often than not present consumer, industrial and sometimes public safety threats that must be called out prominently in documents like this one.	Delete "potentially" in line 280. In line 281, replace "secure and resilient" with "safe, secure and resilient."
2	Andrew Ginter, Waterfall Security Solutions	Major	Entire Document	My comment #1 does not only apply to the Introduction, but the entire document	Review the entire document and consistently call out "safety" as the number 1 threat for control-capable IoT devices. Add examples throughout the document like those I provided in comment #1 to highlight the importance of this issue.
3	Andrew Ginter, Waterfall Security Solutions	Major	Line 292	Line 289 says the report does not focus on safety or privacy, but the paragraph at line 292 then talks about privacy and provides a diagram for privacy concerns	Add a corresponding paragraph on safety Safety is enormously more important to consumers and society than privacy. Unfaithful spouses may launch class actions against automobile manufacturers if automobiles leak information to their faithful spouses that reveal their philandering behavior. But that is *nothing* compared to the outrage that will result from the national disaster described in my comment #1
4	Andrew Ginter, Waterfall Security Solutions	Minor	Line 334	"interact" is too weak. This document should consistently call out "monitoring" activity as different from and much less dangerous than "control" activity. Monitoring produces data, which represents an IT-class threat. Unauthorized and incorrect control is frequently physically dangerous to consumers and others.	Replace "interact" with "monitor and control"

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
5	Andrew Ginter, Waterfall Security Solutions	Major	Line 346-348	The provided list omits "control" and so ignores the single most dangerous physical aspect of IoT devices.	Replace "…processing, sensing, and supporting" with "…processing, sensing, controlling, and supporting."
6	Andrew Ginter, Waterfall Security Solutions	Major	Line 346-348	The provided list omits "control" and so ignores the single most dangerous physical aspect of IoT devices.	Replace "…processing, sensing, and supporting" with "…processing, sensing, controlling, and supporting."
7	Andrew Ginter, Waterfall Security Solutions	Minor	Line 500-501	Nothing is secure. All software can be hacked. To say "are digitally signed to guaranteed their integrity and authenticity" is factually incorrect and misleading. Would you bet your life that a given software implementation has no zero-day vulnerabilities in it?	Replace the offending phrase "are digitally signed to provide a limited degree of confidence in their integrity and authenticity."
8	Andrew Ginter, Waterfall Security Solutions	Major	Line 505-507	This paragraph talks about "privacy and security" but fails to mention major consumer safety challenges. Yes people care if thieves can intercept leaked stovetop usage information to determine when it is safe to break into a house. But people care enormously more that their house does not burn down because their stove is hacked by a terrorist organization.	Replace the offending paragraph with: "Significant safety and privacy challenges associated with both of these projects remain, including the design of communications technology that is physically incapable of compromising correct control of a vehicle from a compromised or malicious BSM or other transmitter, as well as the implementation and governance of a central Certificate Authority."
9	Andrew Ginter, Waterfall Security Solutions	Major	Line 540-541	Forgot "safety" again. Consumers will certainly be reluctant to embrace IoT technology in the home if they feel their safety is at risk.	Replace "if they feel their privacy and data are at risk" with "if they feel their safety and privacy are at risk."
10	Andrew Ginter, Waterfall Security Solutions	Major	Line 564-566	Again, the selected example does not reflect consumers' true priorities.	Replace "by planting backdoors to create and launch an IoT distributed denial-of-service (DDoS) attack" with "by planting backdoors to turn on stovetops at random times, or manipulate both furnaces and carbon-monoxide detectors to asphyxiate residents"
11	Andrew Ginter, Waterfall Security Solutions	Major	Line 569	Forgot "safety" again	Replace "privacy and data" with "safety and privacy"

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
12	Andrew Ginter, Waterfall Security Solutions	Major	Line 717	Nothing is "secure." All software has bugs. Some bugs are vulnerabilities. Therefore all software can be hacked. To say "…it becomes imperative to assure the identity of the "things" in order to have secure exchanges of information" is factually inaccurate – there is no such thing as "secure exchanges of information" and no amount of identity management changes the fact that all cryptosystems and their implementations have serious discovered and undiscovered vulnerabilities.	Replace the offending statement with ""…it becomes imperative to assure the identity of the "things" in order to develop at least limited confidence in the safety of exchanged information. Additional safety standards for control-capable "things" that render such "things" physically incapable of issuing unsafe physical commands are urgently needed."
13	Andrew Ginter, Waterfall Security Solutions	Major	Line 748-749	Encryption is no panacea. Encryption provides a degree of protection against MIM attacks, but no protection against cryptosystem, operating system and other software vulnerabilities. Encryption also provides no protection from compromised endpoints. Cryptosystems encrypt attacks from compromised endpoints just as happily as they encrypt legitimate communications from those endpoints.	Replace "Some existing security controls and practices—such as encrypting wireless data transmissions—can serve to protect AR system inputs and outputs" with "Some existing security controls and practices—such as encrypting wireless data transmissions—can provide a degree of protection for AR system inputs and outputs"
14	Andrew Ginter, Waterfall Security Solutions	Major	Line 763-841	Encryption is no panacea. Encryption provides a degree of protection against MIM attacks, but no protection against cryptosystem, operating system and other software vulnerabilities. Encryption also provides no protection from compromised endpoints. Cryptosystems encrypt attacks from compromised endpoints just as happily as they encrypt legitimate communications from those endpoints. Compromised endpoints can send encrypted messages to carry out unsafe control of physical components putting worker, consumer, public and environmental safety all at risk, depending on the context and extent of the physical processes involved.	Qualify every claim for encryption in this section. And add a section on software vulnerabilities and the gross insufficiency of encryption and identity management as assurance for safe control. Eg: replace the first paragraph with: Cryptographic techniques provide a degree of security to IoT data and transactions, and some benefits as well to ensuring safe and reliable control of physical systems. Cryptographic techniques and mechanisms and their associated standards provide, to a degree: confidentiality, entity authentication, non-repudiation, key management, data integrity, trust-worthy data platforms, message authentication, and digital signatures. Make comparable changes to every claim in this section that "encryption provides X" or "assures Y". Add a paragraph something like "While encryption and cryptographic identity management is indispensable in most IoT designs, cryptosystems have fundamental limitations that IoT designers must take into consideration. Almost all cryptosystems are software, and all software has both discovered and undiscovered vulnerabilities. The mathematical algorithms that are the foundation of cryptosystems are from time to time broken, rendering entire cryptosystems suddenly inadequate to their task. In addition, cryptosystems and identity management do nothing to protect against attacks from compromised endpoints, such as for example, a compromised home automation controller issuing encrypted commands to turn on a stovetop at 2 AM.

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
15	Andrew Ginter, Waterfall Security Solutions	Minor	Line 844-845	The paragraph betrays a lack of imagination as to the possible extent and consequences of cyber attacks.	Replace with: Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident, and where possible, recover from any losses as a result of the incident. In data-centric and monitorinc-centric IoT systems such recovery often includes restoring data from backups. In IoT control systems, recovery can be impossible – human lives cannot be "restored from backups."
16	Andrew Ginter, Waterfall Security Solutions	Major	Line 902-904	Again, nothing is "secure." Only people who sell stuff use "secure" as an adjective to describe their wares. People who have bought a bill of goods also use "secure" as an adjective or adverb. If this report seeks to be credible, we must avoid the use of the word in this way.	Replace the first line in the paragraph with: Identity and access management and related standards provide a degree of security and interoperability for digital identities and attributes of entities to be used across security domains and organizational boundaries.
17	Andrew Ginter, Waterfall Security Solutions	Major	Line 1061	Network connectivity of any sort to safety-critical components is a serious risk that is not addressed in this section.	Add a paragraph: Direct or indirect network connectivity with IoT components controlling potentially-dangerous physical components, whether stove-tops, automobiles or undersea well-head blow-out preventers, poses an additional and serious risk. All software can be compromised, every network message, encrypted and authenticated or not, can encode an attack, and all compromised CPUs can be made to issue every physically unsafe control the CPU is physically able to issue. IoT safety standards urgently require additional development. Safe designs are possible – for example a stove-top controller could consist of two CPUs, one of which controls the stove-top and animates the user's touch-screen, and the other is physically able only to monitor stove-top usage, and communicates with home-automation networks and the Internet. Compromise of the network-exposed "expendable" CPU therefore poses no safety threat to consumers. Unidirectional gateways or their IoT equivalents can facilitate communication between reliability-critical and safety-critical control components and external systems, enabling monitoring of those important subsystems, without the physical possibility of remote attacks or unsafe remote control. Industrial standards such as IEC 61508 are relevant to this new IoT safety standards development effort.

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
18	Andrew Ginter, Waterfall Security Solutions	Major	Lines 1236-1239	The provided definition of cybersecurity is the classic IT/data-centric definition. A new control-centric definition is starting to be used for control-capable devices, a definition that is a "dual" of the data-centric definition. Data-centric proponents argue that all control messages are data, and so protecting data is sufficient to prevent unauthorized or incorrect control. Control-centric proponents argue that when computers control the data, preventing mis-control of those computers protects the data. Both definitions should be referenced in this document, to give readers and practitioners insight into the control-centric view that is essential to safe and reliable IoT control of physical processes.	Replace "Cybersecurity is defined as the prevention of damage to, unauthorized use of, exploitation of, and—if needed— the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems" with The data-centric definition of cybersecurity is "the prevention of damage to, unauthorized use of, exploitation of, and—if needed— the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems." The control-centric definition is "the prevention of unauthorized and incorrect control of electronic information and communication systems, in order to increase assurance of safe and reliable operations of the physical systems those electronic systems control."
20	Andrew Ginter, Waterfall Security Solutions	Major	Lines 1245-1249	The priorities box is data-centric. Add the control-centric dual.	Add Safety: Preventing unauthorized or incorrect control leading to unacceptable risk of human casualties or damage to property or the environment. Reliability: Preventing unauthorized or incorrect control leading to incorrect or non-operation of physical systems.
21	Andrew Ginter, Waterfall Security Solutions	Major	Line 1264	The diagram relegates control functions and risks to "control systems" when in fact there are significant and unacceptable "control" risks in other areas including buildings, consumer & home, healthcare life & science, industrial, transportation and public safety.	Delete the diagram – it sends entirely the wrong impression
22	Andrew Ginter, Waterfall Security Solutions	Major	Line 1267-1278	The DoD CIO quote is data-centric. Replace with a control-centric quote that does not conflate physical safety and reliability issues with "protecting the data" – as if encryption was the answer, what was the question?	Consider using this quote instead, from the Industrial Internet Consortium Security Framework document: "IIoT organizations must place increased importance on safety and resilience beyond the levels expected in many traditional IT environments. IIoT systems may also have data flows that include intermediaries and involve multiple organizations, requiring more sophisticated security approaches than, for example, link encryption. Unfortunately, IT departments rarely speak the same language as those concerned with control systems and OT. The two perceive risk differently, and they cannot be combined for positive gain without a balanced consideration of their differing motivations."

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
23	Andrew Ginter, Waterfall Security Solutions	Major	Line 1330-1340	This paragraph characterizes risk for low-impact, high-frequency events. For such risks there are past statistics that can be used to estimate future likelihood. Consumers and societies care about high-impact, low-frequency events as well, such as the stovetop compromise or automobile compromise disasters in my comment #1. For such events, there are no reliable statistics, and qualitative assessments are notoriously subjective.	Replace the paragraph with something like: For the purposes of this Report, risk is a measure of the extent to which an entity is threatened by a potential circumstance or event. Low-impact, high frequency (LIHF) risk is typically measured as a function of: (i) the adverse impacts (both inherent and residual) that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. High-impact, low-frequency (HILF) risk, for example due to high-capability cyber attacks, cannot be so measured, since there is no way to estimate the frequency of such attacks. Instead, HILF risks due to deliberate attacks are often subjected to a capabilities-based assessment, where a central authority, such as an enterprise or government, issue a Design Basis Threat assessment, requiring that all threats with unacceptable consequences, up to a certain capability level, be defeated reliably. Assessing risk requires the careful analysis of threat capability information, as well as both accidental and systematic / design vulnerability information to determine the extent to which cyber or physical attacks could adversely impact an organization and the confidence the organization has that attacks with truly unacceptable consequernces are reliably defeated.
24	Andrew Ginter, Waterfall Security Solutions	Major	Line 1362-1365	Need to add the control-centric dual into this very data-centric analysis.	Replace with: A threat is any circumstance or event with the potential to induce unacceptable consequences for people, the environment, an organization or the Nation via unauthorized and incorrect control of physical operations via a cyber system, or unauthorized access, hestruction, disclosure, or modification of information, and/or denial of access to that information.
25	Andrew Ginter, Waterfall Security Solutions	Major	Line 1385	Cannot use “secure” as an adjective. See my comment #16	Need to rephrase Confidentiality and Availability requirement. Arguably all 3 of these requirements are redundant though – see my comment #26 below.
26	Andrew Ginter, Waterfall Security Solutions	Major	Line 1385	Missing safety & reliability requirements.	Add the following, and consider removing Confidentiality, Integrity and Availability requirements entirely since they are lower priority than safety and reliability. Safety: V2V, V2I and V2X communications must be physically incapable of causing unacceptable risks of unauthorized or incorrect control of the vehicle Reliability: V2V, V2I and V2X communications must be physically incapable of causing unacceptable risks to continued, correct operation of the vehicle

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
27	Andrew Ginter, Waterfall Security Solutions	Major	Line 1410	Need more safety / reliability examples	Add: • Rendering the car undriveable, for example by erasing all drive-by-wire firmware • Physically damaging engine or other components, for example by constantly applying a degree of braking pressure during normal operations
28	Andrew Ginter, Waterfall Security Solutions	Major	Line 1472	Missing safety threats due to compromise via the BSM communications channel	Add: • An attacker transmits messages on BSM communications channels that exploit vulnerabilities in cryptosystems, operating systems or other software, pivoting through those systems into safety-critical automobile automation components
29	Andrew Ginter, Waterfall Security Solutions	Major	Line 1476	Table is missing “safety” and “reliability” entries	Add: • Safety: Control-capable consumer IoT systems require strong assurances of correct and authorized control of physical processes whose mis-operation could result in unacceptable physical consequences • Reliability: Control-capable consumer IoT systems require strong assurances of continuous correct control of physical processes whose failure represents an unacceptable consequence
30	Andrew Ginter, Waterfall Security Solutions	Major	Line 1544	Table is missing “safety” and “reliability” entries. The “Availability” and “integrity” entries incorrectly conflate data centric with control-centric requirements.	Replace “Availability” requirement with “Health IoT requires that patient information is available to authorized entities when it is needed.” Replace “integrity” requirement with “Health IoT requires the protection of patient information from unauthorized changes that might impair diagnosis or treatment” Add: • Safety: Health IoT requires the protection of patient safety from unauthorized or incorrect control of medical devices • Reliability: Health IoT requires that medical devices control functions work, correctly and when needed
31	Andrew Ginter, Waterfall Security Solutions	Major	Lines 1591-1630	See my comments #29 & 30 and apply here	

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
32	Andrew Ginter, Waterfall Security Solutions	Major	Lines 1633-1634	Need Safety & Reliability requiremens	Add: • Safety: Smart Manufacturing requires that physical manufacturing processes be protected from unauthorized or incorrect control • Reliability: Smart Manufacturing requires that physical manufacturing processes be protected from unscheduled interruption
33	Andrew Ginter, Waterfall Security Solutions	Major	Line 1967	Missing section on “System Safety Engineering”	Add: There are many engineering standards for safety systems, but fewer for how safety systems engineering interacts with cyber security issues. There is very little standards activity describing how to classify IoT systems as to potential safety issues, nor how to engineer IoT systems that are adequately secured in the face of attack surface increases due to network interconnectivity.
34	Andrew Ginter, Waterfall Security Solutions	Major	Lines 1999-2001	Need to mention safety and reliability, not just data-centric priorities	Replace “Risk assessments need to be based upon an IoT application’s priorities for confidentiality, integrity, and availability of information, and for control-capable IoT applications, priorities for physical safety and reliable physical operations.”
35	Andrew Ginter, Waterfall Security Solutions	Major	Line 2038	Missing “System Safety Engineering”	Add: Need to create system safety engineering standards for IoT components, especially consumer-grade components where safety issues are currently poorly addressed.
###					