April 17, 2018

VIA EMAIL: NISTIR-8200@nist.gov

National Institute of Standards and Technology
Attn: Information Technology Laboratory
100 Bureau Drive (Mail Stop 8900)
Gaithersburg, MD 20899-8900

Re: Comment of GuardKnox to NISTIR 8200 (DRAFT)

GuardKnox, a private company specializing in automotive cybersecurity solutions, submits this comment in response to the Request for Comments ("RFC") issued by the National Institute for Standards and Technology ("NIST") on February 14, 2018. The RFC seeks input and feedback on the draft *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things* ("Report"). NIST issued the Report in order to "inform and enable policymakers, managers, and standards participants as they seek timely development of and use of cybersecurity standards in IoT components, systems, and services."[1] GuardKnox believes the Report is an important step in developing IoT standards and appreciates the opportunity to provide input to NIST regarding Connected Vehicles ("CV").

Overall, while GuardKnox welcomes the Report's discussion of CVs as part of the IoT ecosystem generally, we provide two recommendations: (1) that NIST expand the Report's discussion and analysis of CV cybersecurity due to the physical harms that can arise from a compromised CV, similar to the Report's approach to Health IoT; and (2) that NIST cite to specific IoT standards related to vehicle cybersecurity, rather than general standards, so that stakeholders can look to the correct cybersecurity standards when developing and implementing CV technology.

Below, we provide a brief overview of GuardKnox and our technology, followed by a discussion of each recommendations noted above. We note at the outset that these comments are intended to address both CV cars and trucks, as described further below.

I. GuardKnox Overview

GuardKnox is an automotive cybersecurity provider that develops solutions to protect connected vehicle users from threats that can endanger their physical safety and personal

[1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NISTIR 8200 (DRAFT), INTERAGENCY REPORT ON STATUS OF INTERNATIONAL CYBERSECURITY STANDARDIZATION FOR THE INTERNET OF THINGS (IOT), p. iii (Feb. 2018), https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf ("*Report*").

information. Our team members have over two decades of experience in providing hardware and software-based cybersecurity solutions to the Israeli Air Force and its platforms (*i.e.* airplanes). Our team is committed to supplying solutions which protect the automotive industry from the most critical cyber threats.

GuardKnox has substantial experience in fighting the growing cybersecurity threats to CVs and hopes to leverage this Report as we continue to build our CV solutions. Our approach to CV cybersecurity – Communication Lockdown™ – utilizes a fully deterministic system, which ensures the vehicle functions properly.[2] This patented approach does not rely on cloud-connectivity nor call for ongoing updates so malware cannot sneak in and corrupt the CV. Instead, we use security in depth-layered protection to create a fully updateable and verifiable model that enforces predetermined states and keeps internal network communication intact.[3] For example, when a message is sent to a vehicle, GuardKnox technology verifies that the content and source of the message are legitimate at three different layers: (1) the routing layer; (2) the content layer; and (3) the contextual layer (*i.e.*, a state machine).[4] Through this three-layered approach, the CV's communications remain secure, assuring the safety of the CV, its passengers, and pedestrians.

GuardKnox's Communication Lockdown™ does not prevent the OEM from updating the internal network or from having the benefit of new revenue streams that arise for the CV. GuardKnox instead provides an approach that promotes cybersecurity as a foundation of the CV. We believe this approach and our experience makes GuardKnox uniquely situated to provide these comments to NIST regarding the security of the IoT and the CV marketplace. We hope that stakeholders across the industry use this Report to improve their technology and that the Report leads to an increase in overall CV and IoT safety.

II. The NIST Report Should Expand the Physical Harm Discussion Associated with a Compromised Vehicle

GuardKnox believes that the Report should include additional discussion and analysis of the potential physical harms associated with CVs. We note that the current draft of the Report contains general statements on this topic. For example, the Report states that, "[g]reater emphasis [on driver and passenger] safety may be required due to the increased attack surface from V2V,

---

[2] *See* GuardKnox Cyber Technologies Ltd., *Automotive Cyber Security vs. Traditional IT Cyber Security* (Mar. 6, 2018), https://blog.guardknox.com/automotive-cyber-security-vs.-traditional-it-cyber-security*; see also* GuardKnox Cyber Technologies Ltd, *Methodology* (last visited Mar. 20, 2018), https://www.guardknox.com/methodology/.

[3] *Id.*

[4] *See* GuardKnox Cyber Technologies Ltd, *Methodology* (last visited Mar. 20, 2018), https://www.guardknox.com/methodology/.

V2I, and V2X communications."[5] The Report further acknowledges that "severe safety consequences to vehicles and people require risk assessments to be developed."[6] These observations provide some context surrounding the potential for physical harm to arise from cyber-compromised CVs, but lack sufficient detail that would be necessary to highlight the importance of strong CV cybersecurity to counteract such potential harms.

To that end, we recommend that the Report address *how* increased CV cybersecurity and adequate risk assessments can reduce physical harm or risk of death to passengers, drivers, and pedestrians. One option might be to expand on the discussion surrounding Basic Safety Messages ("BSM") and sensor threats by providing explicit, real-world examples of the consequences of weak cybersecurity in the CV context.[7] We appreciate that NIST recognizes threats to cybersecurity may allow an attacker to alter, intersect, or disable the CV's BSM feature or sensors thereby causing (1) unintended disclosure of sensitive information, (2) "unexpected and unsafe" vehicle operation, and/or (3) "harm to passengers and passersby."[8] However, the Report would benefit from expanding on or providing explicit examples of "unexpected and unsafe" or "harm to passengers and passerby"[9] since a faulty BSM or sensor can cause the vehicle to crash into another vehicle, pedestrian, or crowd, resulting in serious bodily injury or death. Indeed, we encourage NIST to acknowledge the potential for increased physical harm that could be associated with cybersecurity attacks that target connected trucks. For example, if a connected truck carrying hazardous materials malfunctions or crashes, the malfunction or crash could lead to a greater amount of physical harm or death than a passenger vehicle. Framing the CV discussion in the Report this way would help readers understand the unique aspects of and risks presented by CVs as distinct from the more general issues raised by other IoT sectors.

In updating the draft Report with additional CV-specific context and analysis, NIST would be mirroring the Report's discussion of physical harms associated with compromised Health IoT and the need to distinguish these harms from other harms associated with the IoT, such as privacy violations.[10] With respect to Health IoT, the Report notes, "medical devices…are unique. In addition to data security and privacy impacts, patients may be physically affected (i.e., illness, injury, death) by cybersecurity threats and vulnerabilities of medical devices...[and] [a]s a result, addressing the…*safety risks posed by cyber threats are of paramount importance* (emphasis

---

[5] *Report* at 37.

[6] *Id*.

[7] *See id.* at 9-10; 37-39.

[8] *Id.* at 37-38.

[9] *Id.* at 38.

[10] *Id*. at 42.

added)."[11] We suggest that CVs, like Health IoT, give rise to "safety risks posed by cyber threats that are of paramount importance." GuardKnox believes if NIST highlights the risk of physical harm and addresses how increased cybersecurity can reduce the potential for physical harm or death, then stakeholders will place more attention towards CV cybersecurity and that consumers will benefit from this increased attention.

III. The NIST Report Should Reference and Discuss Specific Standards Related to Vehicle Cybersecurity

GuardKnox recommends that the Report reference and discuss specific examples of vehicle cybersecurity standards that have already been developed and deployed in the CV space in order to enhance the utility of the Report for stakeholders working on developing CV technology.

On a general level, the Report offers an informative synopsis of the availability and adoption of existing IoT cybersecurity standards by stakeholders across the various IoT marketplaces.[12] However, the Report can go further in referencing existing vehicle cybersecurity safety standards that would be important for stakeholders to review as they develop CV technology. We believe that without referencing existing ***vehicle*** cybersecurity safety standards in the Report, stakeholders may rely on the wrong cybersecurity standards when developing CV technology. This is particularly true when, for example, the Report cites to general "SAE" and "ISO" standards but does not specify particular SAE or ISO standards most relevant to CVs. To address these issues, GuardKnox recommends that NIST include in the Report a discussion of the following standards: (1) *SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* ("SAE J3061"); and (2) *ISO 26262: Road vehicles – Functional Safety* ("ISO 26262"). We also recommend that the Report expand on *ISO 15408: Information technology -- Security techniques -- Evaluation criteria for IT security* ("ISO 15408") and highlight its importance to CVs.[13] We briefly review each in turn, below.[14]

---

[11] *Id.*

[12] *See e.g., Report* at 53-54.

[13] Although NIST need not specifically reference the European Union Agency for Network and Information Security ("ENISA")'s *Cyber Security and Resilience of smart cars: Good practices and recommendations*, GuardKnox believes ENISA's study can provide NIST an informative background on the EU's approach to CV cybersecurity. *See* European Union Agency for Network and Information Security, *Cyber Security and Resilience of smart cars: Good practices and recommendations* (Dec. 2016), https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

[14] We note here that GuardKnox is an active member of both of the standards developing organizations ISO and SAE discussed in this section, participating in Israel and abroad – and we continue to rely on existing SAE and ISO standards when developing and implementing CV technology.

SAE J3061 establishes a set of high-level guiding principles for cybersecurity as it relates to cyber-physical vehicle systems.[15] Specifically, these principles include:

(1) Defining a cybersecurity lifecycle process framework that manufacturers can tailor and incorporate into each stage of the vehicle's software development and implementation, from concept through production, operation, service, and decommissioning;
(2) Providing information related to common tools, methods, and guidance for designing, verifying, and validating a vehicle's cybersecurity; and
(3) Providing a foundation for developing future vehicle cybersecurity standards.[16]

SAE J3061 also features additional material in appendices that includes techniques for threat analysis and risk assessment, threat modeling and vulnerability analysis, sample cybersecurity and privacy controls derived from NIST SP 800-53 that may be considered in design phases, and vehicle-level considerations such as good design practices for electrical architecture. The inclusion of an explicit reference and some discussion of SAE J3061 in the Report would offer stakeholders the opportunity to acquire greater detail and guidance on the security considerations unique to the CV marketplace, which is in keeping with the goal of the document that NIST is preparing.

ISO 26262 is an international standard intended to be applied to safety-related systems in production automobiles "that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3,500 kg."[17] The standard adapts a previously issued IEC standard, and expressly encompasses future mobility technology that CVs represent. In its introduction, the ISO document drives home this point by stating that:

> Safety is one of the key issues of future automobile development. New functionalities not only in areas such as driver assistance, propulsion, in vehicle dynamics control and active and passive safety systems increasingly touch the domain of system safety engineering. Development and integration of these functionalities will strengthen the need for safe system development processes and the need to provide evidence that all reasonable system safety objectives are satisfied. With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from

---

[15] *See* SAE International, *J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle* (Jan. 14, 2016), https://www.sae.org/standards/content/j3061_201601/.

[16] *Id.*

[17] International Organization for Standardization, *ISO 26262: Road vehicles – Functional Safety* (2011), https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en.

systematic failures and random hardware failures. ISO 26262 includes guidance to avoid these risks by providing appropriate requirements and processes.

ISO 26262 recommends that original equipment manufacturers ("OEMs") and tier 1 suppliers adopt a risk-based approach at each phase of developing a vehicle's software and hardware to ensure the "functional safety" of the vehicle. ISO 26262 defines "functional safety" as the "absence of unreasonable risk due to hazards caused by malfunctioning behavior," and a "functional safety requirement" as the specification of an "implementation-independent" safety behavior or measure, including safety-related attributes.[18] ISO 26262 does not follow a one-size-fits all approach to the development of functional safety requirements. Instead, the onus is on the manufacturers and suppliers to achieve functional safety according to the OEM's safety risk assessment of the vehicle's software and hardware capabilities, an approach that we believe NIST would support based on our understanding of the agency's previous work in these and related areas of standards development.

For example, if the vehicle's head-unit allows for entry and control of the engine (*e.g.* for remote start capabilities), then the head-unit would present a different risk profile versus a more limited head-unit that only provides radio and other entertainment capabilities. As a result, the OEM would be expected to harden the head-unit and other subsystems and address vehicle cybersecurity more aggressively in the former scenario, compared to the latter.

We appreciate that the Report includes ISO 15408 because ISO 15408 provides stakeholders an objective evaluation criteria to verify that a device or system adheres to defined security requirements.[19] To that end, we recommend that the Report expand on ISO 15408 and note its importance and applicability to CVs.[20] For example, GuardKnox particularly appreciates the Common Criteria's Protection Profile ("PP") – *i.e.*, a reusable template that expresses security requirements for a group of related devices or systems[21] – but we are concerned that a PP does not currently exist for CVs. The Report provides NIST an opportunity to collaborate with stakeholders and develop a clear PP for CVs. We feel a clear PP would guide industry in their efforts to create and implement secure CVs and believe that extending the Common Criteria framework to vehicles would be a positive step in improving vehicle cybersecurity.

---

[18] *Id.*

[19] *See e.g.*, United States Computer Emergency Readiness Team, *The Common Criteria* (July 5, 2013), https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria.

[20] *See e.g., Report* at 110 ("[Diabetes Technology Society Standard for Wireless Device Security] leverages ISO 15408 to help developers identify and document, using the ISO 15408 standardized framework, the threats applicable to medical device products and components."). GuardKnox recommends further discussion of this nature.

[21] *See e.g.*, United States Computer Emergency Readiness Team, *The Common Criteria* (July 5, 2013), https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria.

IV. Conclusion

GuardKnox thanks NIST for the opportunity to provide this comment and provide recommendations for improvement of the draft Report. We look forward to engaging with NIST to further advance efforts to create and promote safe CV cybersecurity standards. Should you have any questions regarding our comment, please contact Moshe Shlisel at moshe@guardknox.com.

Sincerely,

/s/ Moshe Shlisel, CEO, GuardKnox

COMMENT #	SOURCE	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	GuardKnox Cyber Technologies Ltd.; 2 Hahazon Street, Ramla, Israel; moshe@guardknox.com cc-jillian.goldberg@guardknox.com	Major	n/a	GuardKnox believes that the Report should include additional discussion and analysis of the potential physical harms associated with CVs.	GuardKnox recommends that NIST expand on the Report's discussion and analysis of CV cybersecurity due to the physical harms that can arise from a compromised CV, similar to the Report's approach to Health IoT.
2	GuardKnox Cyber Technologies Ltd., (see previous comment)	Major	n/a	GuardKnox believes that the Report provides an informative synopsis of existing IoT cybersecurity standards but should also reference vehicle specific cybersecurity standards.	GuardKnox recommends that NIST cite to specific IoT standards related to vehicle cybersecurity, rather than general standards, so that stakeholders can look to the correct cybersecurity standards when developing and implementing CV technology.