Before the
National Institute of Standards and Technology
Gaithersburg MD 20899-8930

In the Matter of)
)
Report on Strategic U.S. Government) NISTIR 8074
Engagement in International)
Standardization to Achieve U.S.)
Objectives for Cybersecurity)

Comments of Netmagic Associates LLC

Anthony M. Rutkowski
Principal
44441 Blueridge Meadows Drive
Ashburn VA 20147-2895
tel: +1 703.999.8270
mailto:trutkowski@netmagic.com

Filed: 23 September 2015

Summary

i. The NIST technical report is being wrongly used to promulgate significant federal policies, to ascribe far reaching new authority by its authors to themselves, and to superficially meet industry collaboration requirements

ii. The report is one of many similar ones prepared over several decades by USG agencies - indeed governments worldwide. The NIST Report should recognize and consider emulating this extensive array of existing material and recommendations.

iii. Such reports are inherently challenging because of different agency missions, funding, experiences, staff, and political/policy constraints. The NIST challenge here is exacerbated because other USG agencies have far more extensive international cybersecurity standardization missions, ongoing activities, experience and staff - that have existed for many decades.

iv. The international cybersecurity standardization ecosystem and activities - both as to involved USG agencies and international forums - are far more complex and extensive than portrayed in the draft report. Some of the most important agencies, organizations, and activities are simply omitted. Why the NIST draft report failed to include so many of the most important components of the international cybersecurity standardization universe is disconcerting.

v. The objectives of the draft report are not apparent. The material in the report seems to reflect NIST's mission and current activities. Eight recommendations are offered. For the most part, they are largely identical to well-intended exhortations that have existed for decades in every similar report, but have proven difficult to implement for many practical reasons that are unfortunately not treated. A recommendation placing NIST at the helm of all USG interagency coordination to "ensure USG coordination" seems both highly self-serving as well as plainly infeasible. It is part of the problem.

vi. As a first step, a considerably improved understanding is essential about some of the most innovative and important ongoing international industry cybersecurity standardization activities such as the Center for Internet Security's *20 Controls*, the OASIS Technical Committee on Cyber Threat Intelligence, and the global public standardization forums of The MITRE Corporation. The innovation should come from less government-led, more industry-cooperative approaches of which these three are exemplary. The proffered NIST coordination approach is classic government-in-charge. The focus should shift from the government being coordinator of all things cybersecurity to a good buyer and adopter based on a much better understanding of what is occurring across the array of industry forums and the most effective solutions.

vii. Consideration should be given to highly successful new approaches recently undertaken by allied nations such as the U.K., Canada, and Australia, where the principal security assurance body for the nation is given independent recognition, additional responsibilities, and resources related to international cybersecurity standardization. The prominent model is that of the UK's cybersecurity strategy where an ensemble of security assurance, law enforcement, intelligence, and critical infrastructure protection agencies work together with industry in diverse global standards venues in advancing cybersecurity.

1. These comments are filed pursuant Sec. 20(c)(2) of the NIST Organic Act [15 U.S.C. 278g-3(c)(2)], inter alia, and the public notice provided by NIST in conjunction with the publication of draft NISTIR 8074, 10 Aug 2015. We chose not to use the comment templates provided on the NIST site because they are suitable only for minor changes to NIST technical reports, and not to a major national policy making proceeding. The draft NISTIR is de facto a major policy making proceeding raising broad policy issues that are treated in these comments. In addition, the substantive technical and organizational material contained in the NISTIR is so profoundly deficient at this stage, a second draft is plainly needed. See also the Annex to these comments.

2. The commenter is a prominent engineer-lawyer consulting as Netmagic Associates LLC who for the past 40 years has been highly active in senior positions in government, industry, and academia undertaking the subject matter of this NIST Report. In those capacities, he has authored scores of related materials, including similar reports and diagrams within the Federal government and industry going back to the late 1970s.[1] Over the past decade, he has been directly responsible for authoring or leading a large number of the most prominent international cybersecurity standards activities in multiple bodies - both representing private sector companies and on formal U.S. delegations.[2] He is also notably the rapporteur leading joint government-industry preparation of the *Global Cyber Security Ecosystem Technical Report* – a rather large compendium of all ongoing international cybersecurity standardization activities.[3]

[1] *See* Annex B,

[2] *See, e.g.,* ETSI TR 103305 CYBER *Critical Security Controls for Effective Cyber Defence*; ETSI TR 103331 CYBER *Structured threat information sharing*; ETSI TR 103369 CYBER *Design requirements ecosystem*; ETSI TR 103690, *Lawful Interception (LI) eWarrant Interface*; ETSI TR 101567, Lawful Interception (LI), *Cloud/Virtual Services (CLI)* ; OASIS, *Cyber Threat Intelligence (CTI) Technical Committee, Charter,* co-author; ITU-T Rapporteur (2009-2012) for the X.1500 Series Recommendations for *Structured Cybersecurity Information Exchange (CYBEX*).

[3] See Work Item TR CYBER-004, ETSI TR 103306 CYBER; *Global Cyber Security Ecosystem.*

I. The NIST technical report is being wrongly used to promulgate significant federal policies, to ascribe far reaching new authority by its authors to themselves, and to superficially meet industry collaboration requirements

3. The NISTIR 8074 admits at the outset, this document actually constitutes a major U.S. policy making proceeding:

> *This report sets out proposed United States Government (USG) strategic objectives for pursuing the development and use of international standards for cybersecurity and makes recommendations to achieve those objectives. The recommendations cover interagency coordination, collaboration with the U.S. private sector and international partners, agency participation in international standards development, standards training and education, use of international standards to achieve mission and policy objectives, and other issues.*[4]

Indeed, as noted in the Introduction of the NISTIR, the source of the report was not NIST, but an apparently ad hoc the "NSC Cyber Interagency Policy Committee's International Cybersecurity Standardization Working Group."[5] Additionally, the resulting NISTIR is asserted to be "the basis for the required report to Congress" pursuant to Sec. 502 of the Cybersecurity Enhancement Act of 2014,[6] and constituting "a plan for ensuring…interagency coordination in the development of international technical standards related to information system security."[7]

4. Thus, this NISTIR is far more than an ordinary NIST technical report, but rather one that constitutes a highly significant and far reaching policy document submitted to Congress and purports to represent the common views of industry and all government agencies on matters of considerable policy importance. However, the woefully inadequate process by which it was assembled prevents this objective from being met. What is especially disconcerting is how the NISTIR deviates rather significantly from the

[4] NISTIR 8074 Volume 1 (Draft), *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, August 2015 [hereinafter referred to as NISTIR, Report, or NISTIR Report], at iv.

[5] *Id*. at 1.

[6] *An Act to provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes*, Public Law No: 113-274.

[7] *Ibid*.

requirements actually found in Sec.502 of the Cybersecurity Enhancement Act which state:

> *SEC. 502. International cybersecurity technical standards.*
> *(a) In general.—The Director, in coordination with appropriate Federal authorities, shall— (1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and (2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.*
> *(b) Consultation with the private sector.—In carrying out the activities specified in subsection (a)(1), the Director shall* ***ensure consultation with appropriate private sector stakeholders.*** [Emphasis added.]

What in fact seem to have occurred is that the NIST Director outsourced the § 502(a) responsibility to a NSC working group for which there is no record and its members are unknown, and then simply published its report as a NISTIR on a NIST technical publications website to fulfill the § 502(b) responsibility to "ensure consultation with appropriate private sector stakeholders." There is no Federal Register notice of this Report or the ensuing proceeding, or public meeting of any kind – deviating from both the law and Administration policies concerning openness and transparency.[8] These actions fall far short of the Congressional requirement to "ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security," and to "ensure consultation with appropriate private sector stakeholders."

5. The concern over the sufficiency of the process here is exacerbated by two important factors. First is that Recommendation 1 of Report has the authors themselves - the NSC Committee and NIST - unilaterally assuming all major United States international standards policy making and coordination responsibilities, Second is that the draft Report is profoundly insufficient in its portrayal of domestic agency and international cybersecurity standards body activities and forums.

[8] *See Administrative Procedure Act*, 5 U.S.C. § 553. While it is possible to avoid the APA requirements for certain foreign affairs functions, for example involving treaty organizations, the broad scope of the policies being established in the draft Report extend far beyond only treaty organizations. It may be possible to invoke the interpretative rule exception § 553(d)(2), the scale and far reaching effects of the proposed recommendations weight on the side of considerably greater transparency, public notice and comment.

6. The assumption of powers being proposed here is far beyond what is either realistic or appropriate:

> *The U.S. Department of Commerce would host a subordinate interagency working group --the International Cybersecurity Standardization Working Group –on behalf of the EOP interagency policymaking body. Such a group would be comprised of senior Federal cybersecurity officials with the expertise and bandwidth to develop and implement a comprehensive set of objectives and strategies, <u>and to develop and implement a comprehensive set of objectives and strategies, and to coordinate on major issues in standardization before and as they arise</u>. <u>Major policy decisions and areas of significant disagreement could then be brought to the EOP body</u>.*[9] [Emphasis added.]

The enormous breadth and dynamics of the international cybersecurity standardization ecosystem today - where the changes are occurring in forums around the world daily - significantly stresses the resources of even the largest private sector companies in their individual areas of expertise. It is also myriad private sector companies who drive this activity today, not governments. It rather strains credulity for an interagency body to even assert it has the knowledge and competence for the entire universe of cybersecurity to "develop and implement a comprehensive set of objectives and strategies, and to coordinate on major issues in standardization <u>before and as they arise</u>." Not even the most authoritarian countries today would ascribe such omnipotent responsibilities to a Federal Government committee. And, a patent omission is treating the rather key question of how the private sector that drives all this activity even figures into the monolithic interagency committee scheme being proposed.

II. The NIST Report ignores the many similar ones prepared over many decades and which exist today in other venues

7. The subject matter being treated in the instant NISTIR is hardly new. Indeed, international cybersecurity standards activities, roles and coordination among the different agencies and with the private sector - have a well-known history extending back to the early 1920s. At that time, multiple U.S. government agencies had significantly scaled the evolution and U.S. involvement in international network security standards

[9] Recommendation 1, NISTIR Report at 11.

bodies that emerged following World War I.[10] Each agency had an independent mission and authority. The international standardization activity resulted in the creation of what is the most enduring interagency committee in the history of the U.S. government – the Interdepartment Radio Advisory Committee (IRAC) – created on 1 June 1922.[11] In contrast to the NISTIR Report, however, IRAC's role is narrowly constructed and provides for substantial autonomy among the agencies.

8. In the early 80s, the commenter while at the FCC prepared an extensive 67-page report that was subsequently published and became widely used as a teaching reference at the university level.[12] The 1982 report covered many of the same agencies and organizations and treated several issues including the ability to get access to information, to assess U.S. interests - with the reality that involved agencies had independent, autonomous missions and capabilities. The core recommendations of the report were to eschew notions of central control and instead facilitate knowledge and intelligence sharing about what was occurring.

> *It would seem that a better choice of internal reform would lie in the establishment of a broad, multidisciplinary analytical function within the government infrastructure, devoted to international communication issues. Such a function should consist of four components: 1) a current, centralized bibliographic reference center…, 2) an open staff component located in a major responsible agency and sheltered from rigorous bureaucratic entrapments, 3) a closed, dedicated staff component within DDI [CIA Deputy Directorate for Intelligence which at the time had established the innovative National Foreign Assessment Center (NFAC)], and 4) a permanent advisory committee with a mandate to assure diversity.*[13]

In part, the Department of State and Federal Communications Commission subsequently took steps to implement some of these recommendations.

[10] At that time, the networks were largely radio-based, but very much encompassed essentially all the security challenges being faced today. Indeed, the term "cybersecurity" is so broad and abstruse – and very much encompassing radio based networks – that it is interchangeable with network security.

[11] *See* GAO, *The Interdepartment Radio Advisory Committee*, GAO-0-1028, 30 Sep 2004); R.H.Coase, *The Interdepartment Radio Advisory Committee*, Journal of *Law and Economics, Vol. 5 (Oct. 1962); E.M.Webster, The* Interdepartment Radio Advisory Committee, Proceedings of the IEEE, Vol. 33, Issue 8 (Aug 1945).

[12] *See* A.M. Rutkowski, *United States Policymaking for the Public International Forums on Communication*. Vol. 8, Syracuse Journal of International Law & Commerce, 95 (1982).

[13] *Id.* at 144.

9. The Global Cyber Security Ecosystem Report reveals that a considerable number of country reports similar to the NISTIR have been prepared over the past few years.[14] Many of these reports have been tallied as well by NATO and ENISA cooperative cybersecurity centers of excellence.[15] There are no monolith interagency committees.

10. Had the NISTIR drafting committee researched the history of subject matter or examined how other nations are dealing with the identical challenges, it might have avoided the significant inadequacies of the draft Report, as well as the seriously misdirected scheme to establish a monolithic interagency committee "to develop and implement a comprehensive set of objectives and strategies, and to coordinate on major issues in standardization before and as they arise [including] major policy decisions [for all international network security standardization]."

III. Federal agencies have very different international cybersecurity standards making missions, needs, funding, and experiences – many of which are far more extensive than NIST's

11. One of the pervasively enduring challenges of dealing with U.S. government agencies and their respective activities in international standards bodies is that the missions, needs, funding, and experiences tend to be very different. They also tend to be far more extensive than NIST's – which is largely focused only on its own specifications intended for Federal Government use, and largely confined to a single legacy SDO – the ISO – plus a comparative handful of other international standards forums. Remarkably, the NISTIR never identifies U.S. government agencies presently engaged in international cybersecurity standards forums and which presumably would be swept under the control of the proposed new interagency committee. Even a cursory survey of participation in current international cybersecurity standards activities provides a good quantifiable indication of the agencies: the Department of State (DOS), the Department of Homeland Security (DHS), the Department of Defense (DOD), the Department of Justice (DOJ)/ Federal Bureau of Investigation (FBI), the Federal Communications Commission (FCC),

[14] *See Global Cyber Security Ecosystem Technical Report*, *supra*, Annex A.
[15] See Cyber Security Strategy Documents, NATO Cooperative Cyber Defence Centre of Excellence; National Cyber Security Strategies in the World, European Union Agency for Network and Information Security.

the Government Services Administration GSA), The MITRE Corporation (as a FFRDC), the National Geospatial-Intelligence Agency (NGA), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the National Telecommunications and Information Administration (NTIA). Among these agencies, the NSA, DHS, and MITRE clearly have by any measure the most significant level of activities and stature within the international cybersecurity standards making ecosystem. A similar cursory analysis of national cybersecurity strategies of other nations and their treatment of participation of their agencies in international standards forums reveals that their NSA and DHS equivalents, combined with the national telecommunications regulatory authority, are the prevailing participants. However, except in the radiocommunication domain, the FCC as the U.S. telecommunications regulatory authority has not been very active in these forums. Increasingly today in the massively growing Network Functions Virtualization security bodies, it is also the law enforcement authority technical communities (i.e., FBI equivalents) that are active participants.

12. In practice, these expert and participatory U.S. government security agencies work together already today in international cybersecurity standardization bodies – often cooperating with peers and possessing their own global and domestic collaboration mechanisms. The U.S. agencies collaborate as needed with other Federal Government agency participants, within their own agency, and with the private sector. It would be highly counterproductive to subject the agencies to an interagency uber-control of their activities dictated by NIST- which in most cases doesn't begin to possess comparable resources and expertise, and whose mission is entirely different.

IV. The international cybersecurity standardization ecosystem and activities are far more complex and extensive than portrayed in the NIST Report, and some of the most important agencies, organizations, and activities are simply omitted

13. As described above, the cybersecurity standardization ecosystem as it involves U.S. government agencies is complex – which is never even raised or treated in the report. The NSA, DHS, MITRE, and DOJ are significantly engaged and highly respected worldwide. They also collaborate extensively with through counterparts in other nations

on matters before multiple standards bodies. The stature of these activities as well as the "backplane" activities are unrecognized and untreated in the draft Report.

14. Also not treated is the global stature of NIST itself as an international cybersecurity standards body. In some standards domains, NIST's domestic standards for the Federal government are well done. As a result, NIST has been given so-called A.5 status by the principal intergovernmental organization in the cybersecurity ecosystem – the ITU International Telecommunication Standardization sector. This means that its specifications can be cited as international standards, and this has occurred on a widespread basis not only in ITU forums, but also other major global cybersecurity standards bodies such as ETSI, and a considerable number of national level standards bodies worldwide. For reasons that seem to relate to NIST's outdated views on international standards making and enduring affection for ISO, it has failed to be an advocate for its own standards in the global cybersecurity standards ecosystem.

15. It is the identification and treatment of the international forums themselves, however, that are profoundly lacking in the NISTIR – portraying instead a strange decades old perspective on Standards Development Organizations rather than the rather considerably more diverse array of industry forums in which meaningful cybersecurity standards work is done today. The following diagrams graphically display the disparate perspectives.

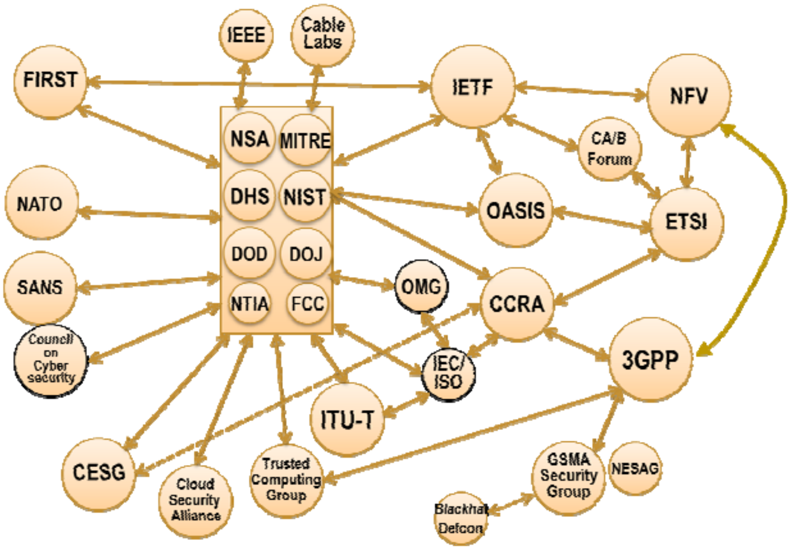

Figure 1 – Actual international cybersecurity standards ecosystem

Figure 1 shows a simplified diagram of multiple current ongoing international cybersecurity forums and activities from a U.S. perspective - based on an analysis of how the principal platforms become created and manifested across the ecosystem through ongoing participatory and collaborative relationships. This depiction has been used and refined in numerous briefings and meetings over the past year domestically and internationally. A version was adopted for the Global Cyber Security Ecosystem Technical Report. By almost any measure, the most widely regarded and used contemporary cybersecurity activities in the ecosystem today revolve around: 1) multiple platform components developed and standardized by MITRE, 2) the *20 Critical Security Controls for Effective Cyber Defense* developed by NSA's Information Assurance Division and now moving forward under the aegis of the Council on Cybersecurity/ Center for Internet Security, ETSI, and multiple national security agencies, and 3) the Cyber Threat Intelligence sharing platforms developed by DHS and MITRE and now proceeding in a dedicated OASIS technical committee. On the horizon, the considerable array of NFV cybersecurity specifications exist in the massively active and fast moving NFV Industry Specifications Group. Also significant is the work ongoing in the Trusted Computing Group, 3GPP SA3 (security), GSMA's Fraud and Security Group, and the CA/B Forum that represent further highly active industry specification development venues making a difference in the industry driven cybersecurity world.

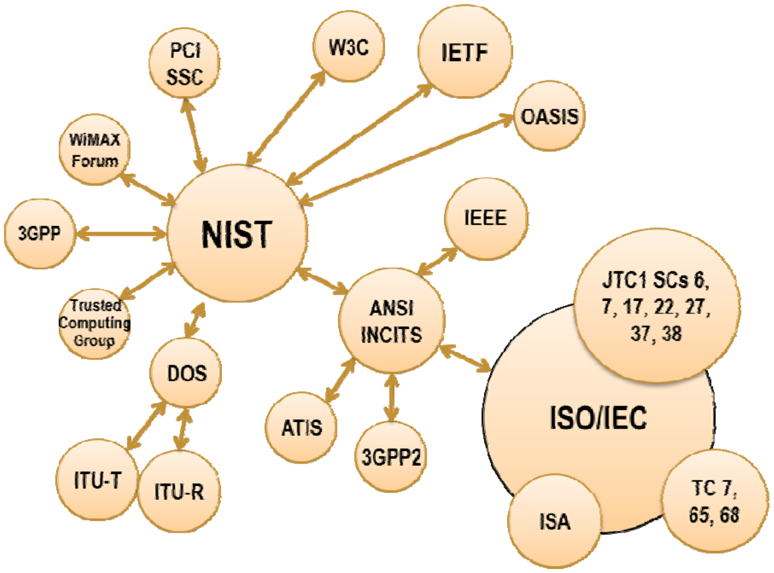

Figure 2 – the international cybersecurity standards ecosystem in the draft NISTIR

By contrast to the broad industry perspective in Fig. 1, Figure 2, above, portrays the NISTIR perspective on the cyber security ecosystem extracted from Vol. 2 of the draft report. It is an entirely different perspective, with a different set of objectives. There are only a few forums mentioned and they are overwhelmingly clustered around the ANSI and ISO/IEC bodies in which NIST predominantly participates. Indeed, the objectives seem largely designed to promote NIST's largely moribund cybersecurity framework and help ANSI-ISO-IEC overcome their fundamental liability - selling unjustifiably high priced process specifications that the industry eschews. Even more embarrassing is that the NISTIR in describing "the U.S. standards strategy" uses what is a 30 year old ANSI promotion of its standards that for years was used to fight the development of Internet standards, and reflects a world that has long disappeared.[16] The collective effect is to dismayingly convey a sense that the NISTIR Report fails fundamentally to understand the international cybersecurity ecosystem for which it is now developing recommendations..

[16] *See* reference to United States Standards Strategy, NISTIR, page 3.

V. NIST Report seems designed to assert broad policy making authority and interagency roles for NIST which are inappropriate

16. The explicit objectives of the draft report are not apparent other than to fulfill a Congressional requirement for a report. As discussed above, most of the material in the report seems to reflect NIST's mission and current activities, and the opportunity has been used to assert an uber-role across the U.S. government for NIST. Eight recommendations are offered.

1. Ensuring USG coordination
2. Promoting USG participation in cybersecurity standards development
3. Developing timely and technically sound standards and assessment schemes for cybersecurity
4. Leveraging U.S. public and private sector collaboration in standards development for cybersecurity
5. Enhancing international coordination and information sharing
6. Supporting and expanding standards training for Federal agency staff
7. Developing technically sound international standards for cybersecurity that minimize privacy risk
8. Using relevant international standards for cybersecurity to achieve mission and policy objectives

For the most part, these well-intended exhortations are similar to almost every report of this nature that has emerged over the past century. One notable if not ironic difference is found in the first recommendation where single agency seeks to denominate itself as a kind of overlord of all U.S. participation in all the diverse international network security activities:

- "to develop and implement a comprehensive set of objectives and strategies
- coordinate on major issues in standardization before and as they arise, and
- [have] major policy decisions and areas of significant disagreement…be brought to the EOP body."[17]

17. Even in long past eras when the technology was much simpler, the bodies were few, and provisioning was by a small set of providers under substantial Federal regulatory control, this kind of assertion of monolithic power never occurred. That it would even be proposed today suggests a certain disconnectedness from today's ecosystem. Indeed, this NISTIR Report and recommendation is itself part of the challenge being faced.

[17] Report, Recommendation 1.

VI. The NIST report should shift its focus away from an omnipotent Federal role in international cybersecurity standards making and reflect the actual industry-led activities existing today

18. As a first step, a considerably improved understanding is essential about today's global cybersecurity ecosystem – what it consists of, how it functions and evolves - which activities and venues are important and which are not. The ancient notion of "SDOs" and their being central to this activity has long been discarded and most progressive nations. The only nation that seems to still maintain allegiance to an SDO-only world is Russia.

19. After nearly a year of private-sector and government activity to develop the Global Cyber Security Ecosystem Technical Report, a consensus was reached that the functioning ecosystem consisted of several hundred identified forums grouped in seven highly interrelated clusters:

1. **Forums that develop techniques, technical standards and operational practices**
2. **Major IT developer forums**
3. **Activities for continuous information exchange**
4. **Centres of excellence**
5. **Reference libraries, continuing conferences, and publications**
6. **Heritage sites and historical collections**

All the different species of cybersecurity standards forums develop, shape, and/or promulgate specifications used in products and services today. If the metrics of participation and "force and effect" of the specifications are quantified, it is decidedly the some of the fast moving, highly adaptable venues in the first cluster, combined with the second cluster, combined with "continuing conferences" in the fourth cluster that decidedly come out on top. It is where most of industry participates – often in the tens of thousands – and where specifications and techniques get driven most immediately into products and services. The intransigent legacy SDOs come out at the bottom and are relegated to handfuls of participants who either do not understand the ecosystem dynamics, or tethered by bureaucratic practice and institutional history to particular venues.

20. What cannot be underscored enough is the degree of dynamics within the ecosystem. In many ways, the global standards environment today resembles the real-time traffic analysis operative in the GoogleMaps application. The participants today with the best strategic capabilities and resources among companies or governments are monitoring all the venues in near real-time, observing who is participating and in what numbers, what subject matter and documents are being input, what significant developments are moving through the often weekly meetings, and what is being published. The major players then tailor their input documents and participation for each meeting to optimize their effectiveness and knowledge base. The old SDOs that meet infrequently among a few people and slowly progress standards over periods of years, and then attempt to sell them – are not even on the relevancy horizon except for a handful of government actors.

21. An example of this dynamic interplay among clusters occurred recently with the discovery of the significant Android OS cybersecurity vulnerability – Stagefright. Within a matter of hours, the company discovering the vulnerability (Zimperium) informed the vendor (Google), filed CVEs in the National Vulnerability Database, distributed threat information within a specialized handset security group, informed the GSMA device security group, and obtained a presentation slot at the Devcon 2015 conference. Within days, these groups in turn prepared patches, technical advisories, and development specifications designed to mitigate the threats posed. At the outer periphery, still other standards groups with longer time constants adjusted their relevant specifications.

22. If one assesses the relative importance of ongoing international industry cybersecurity standardization activities today, it would be the Center for Internet Security's 20 Controls, the OASIS Technical Committee on Cyber Threat Intelligence, the cybersecurity platforms in MITRE standards fora that rank at the top. Second order of importance would include ETSI TC CYBER work items, CA/B Forum platforms, NFV ISG work items, and possibly 3GPP SA3 security assurance specifications. The IETF SACM may still have promise. Almost none of these principal developments are even identified in the draft NISTIR Report. The overwhelming work and innovation in cybersecurity comes from industry-cooperative approaches of which those identified above are exemplary. The proffered NIST coordination approach is classic government-in-charge. The focus should shift from the government being coordinator of all things

cybersecurity to being a good buyer and adopter based on a much better understanding of what is occurring across the array of industry forums and the most effective solutions.

23. The NISTIR Report completely ignores what are key international cybersecurity standards development components today such as developer forums, continuous information exchange, centres of excellence, reference libraries, continuing conferences, publications, and historical collections and heritage sites. Notably the last for the U.S. consists of the Cyber Center for Education and Innovation and Home of the National Cryptologic Museum.[18]

VII. The NIST report should emulate new broadly inclusive government – industry international cybersecurity cooperative activities effectively used by U.S. allies

24. In other countries with comparable marketplace and governance systems, there are government-industry cooperative approaches worth emulating. Prominent examples include the U.K., Canada, and Australia, where the principal security assurance body for the nation is given independent recognition, additional responsibilities, and resources for enhanced to international cybersecurity standardization. Perhaps the best of breed is the UK's cybersecurity strategy arrangement where an ensemble of security assurance, law enforcement and critical infrastructure protection agencies work together with industry in diverse global standards venues to understand what is occurring and advancing cybersecurity.[19]

25. The U.S. also needs a much more effective partnership and resources within its security assurance and intelligence community, including not only the Information Assurance Directorate, but also potentially increased use of the CIA analytical assets – as has occurred in the past – is potentially very useful. This larger role is also consonant with CIA Director Brennan’s recently announced refocus on cybersecurity.

[18] *See* Vision for the The Cyber Center for Education and Innovation and Home of the National Cryptologic Museum (New Museum).

[19] *See* The UK Cyber Security Strategy Report on Progress and Forward Plans, Dec. 2014.

Annex A: Detailed deficiencies in the Report, Volume 2

This annex provides comment on the various sections found in Volume 2 of the draft NISTIR.

1 Why are cybersecurity standards critical?

This section overstates the criticality of standards. Cybersecurity encompasses almost anything and everything related to information communication. Not all of it is "critical," nor is the associated security. Furthermore, the principal challenge for cybersecurity is dealing with all bad code waiting to be discovered or exploited. Standards can only deal with parts of that challenge, and are certainly not in themselves a solution. Consider that the platform generally regarded as the most secure is Apple iOS – and little is standards based.

2 Why is conformity assessment for cybersecurity standards important?

Here also, the importance of conformity assess for cybersecurity standards is overstated, and in general has not proven to be especially useful in enhancing cybersecurity – notwithstanding Lard Kelvin's 1883 pronouncement. The marginal usefulness of conformity assessment seems rather apparent considering most cybersecurity problems arise from coding mistakes, exploits, insider threats, and attacks on equipment and infrastructure after it has been operational. Furthermore, given the rapid rate of development of new hardware and software, it isn't apparent how conformance assessments would be applied and or what standards would be used.

3 Core Areas in Cybersecurity Standardization

The ten areas listed are important but not in themselves a useful tabulation. Focus should be shifted to the 20 controls promulgated by the Council on Cybersecurity (and many other Information Assurance agencies worldwide) and the exchange of structured threat information being advanced by the Department of Homeland Security and multiple other cybersecurity standards forums.

4 Some Key IT Applications

The six sectors listed are important (and perhaps not coincidentally identical to areas of focus by NIST). There are many others, however, that seem ignored. These include, for example the vast and rapidly expanding world of mobile communications and applications, Network Functions Virtualization (NFV) that will constitute the basic infrastructure for future communication infrastructure, and the entire domain of network forensics necessary for dealing with cybersecurity, cybercriminal, and cyberterrorism threats.

5 Present State of International Cybersecurity Standardization

This section seems highly skewed around core areas of interest to NIST in conjunction with its missions and SDOs with which it deals – principally ANSI-ISO-IEC. It notably omits the sectors mentioned above.

6 Standards Developing Organizations (SDOs)

Here also, this section portrays an ecosystem conforming to the narrow segment of international cybersecurity standards activities of interest to NIST. It largely reflects a world that existed two decades ago.

7 IT Standards Development

Here also, the development process reflects the activities of interest to NIST and a world that existed two decades ago. By comparison, it is worth consulting the Global Cyber Security Ecosystem Technical Report and its treatment of the venues and how standards are developed today.

Also not treated is the key factor of availability of standards. The formal legacy bodies that NIST tends to favor operate in very closed and rigid forums, and do not make their standards freely available. As a result, the standards cost thousands of dollars to even see the complete sets, take long periods to prepare, and are generally rejected by industry today.

8 Accelerating IT Standards Development

In light the of reality that most of the viable international cybersecurity standards activity today occurs overwhelmingly through the private sector, it seems surreal to be suggesting that an interagency committee could somehow make it occur. The decades old examples provided are not viable today.

What should be considered are contemporary examples that have successful such as: 1) DHS/MITRE in the case of Cyber Threat Intelligence exchange, 2) NSA's IAD in the case of the 20 controls via the Council on Cybersecurity and multiple other bodies, and 3) the UK Home Office and counterparts in the case of forensics acquisition security especially for NFV.

9 Ongoing Issues in IT Standards Development

This section seems to contain an incoherent set of rambling statements and assertions that have little or no relevance to international cybersecurity standards. It is also incomprehensible and inexcusable that a purported statement of "United States Standards Strategy" is actually a link to an ANSI public relations page to sell its services. It is also preposterous to be asserting that the U.S. is somehow unique today in its approach to network security standards. Most nations are facing the same challenges.

10 How to Effectively Engage SDOs

This section reads like it was written two decades ago. What seems plainly needed is a considerably better understanding of what international cybersecurity forums actually exist today, which are the most active and relevant, and how to participate in the activities given the comparatively small Federal agency resources. It is a decision to be made largely by individual agencies based on their missions and budgets.

Annex B: Qualifications of Anthony M. Rutkowski

For more than a decade, Rutkowski has participated in both leadership and contributory roles in a broad array of international standards and industry bodies dealing with Cybersecurity, Lawful Interception, Retained Data, Critical Infrastructure Protection, and Identity Management. Since 2009, he has served as Executive VP for Industry Standards and Regulatory Affairs at Yaana Technologies LLC of Milpitas California and Yaana Limited of London, England. Over that period, his contributions included many hundreds of written input contributions, reports, and presentations in scores of international security standards fora. As these activities over the past several years have migrated to Cloud Computing and then Network Function Virtualization environments, his work has shifted to these activities and the principal industry forums. This activity includes currently serving as the rapporteur for the ETSI Cloud Computing and Virtualisation Technical Report and a leading contributor NFV LI and RD platform development.

He is also the rapporteur for four ongoing cyber security technical reports in the ETSI Cyber Security Technical Committee. From 2009 to 2012, he also served as the rapporteur for Electronic Warrants, and Rapporteur for Cybersecurity work in ITU-T that included X.1500 and a dozen specifications for structured information exchange.

He is an BSEE engineer-JD lawyer who has pursued a 45 year multifaceted career as a highly visible and well-known global enterprise strategist, public official, organization leader, consultant, lecturer, and author in both the Internet and telecom worlds, in the U.S. and internationally. He is also a Distinguished Senior Research Fellow, at the Georgia Institute of Technology Nunn School where he occasionally lectures on cybersecurity developments.

From 2000-2009, he was Vice-President for Regulatory Affairs and Standards at VeriSign, Inc. In that capacity, he developed, coordinated, filed, and articulated VeriSign regulatory and strategic technical interests in governmental and industry forums worldwide, as well as provided product development and regulatory counsel to the company and government customers. Previous positions include the private sector (VeriSign, SAIC, General Magic, Sprint International, Horizon House, Pan American Engineering, General Electric, Evening News Association) government (Federal Communications Commission, the International Telecommunication Union, Cape Canaveral City Council), academic (Georgia Tech, Internet Society, MIT, and NY Law School), and consulting both as NGI Associates.

Over recent years he has been part of such diverse activities appointment to the Chair of the ITU-T Focus Group on Identity Management Requirements Working Group (2007), ITU High Level Experts Group on Cybersecurity (2007), FCC WARN Act Advisory Committee to develop a next generation emergency warning system (2006), annual keynote speaker at the Intelligence and Surveillance Systems conferences (2002-2006), rapporteur for the European Union Retained Data standard (2006), Chair of the OASIS Legal XML Subscriber Forensics Group (2003), Guest Editor of the IEEE Internet Computing special Millennium Edition; co-producer of the Global Next Generation Internet Conference, and a columnist for Communications Week International (2000).

He co-founded diverse international organizations: Global Lawful Interception Industry Forum (2002), the Agent Society (1996), the Internet Law and Policy Forum (1995), the International

WWW Conference Committee (1994), the Internet Society (1991). He has participated in Internet projects preparing reports by the Aspen Institute, the Rand Corp, the International World Wide Web Conference Committee (Board), Register of Copyrights, the President's Framework for Global Electronic Commerce task force, and the Harvard Kennedy School GII Project. Featured twice in the Washington Post, and listed in the 1996 roundup issue of Inter@ctive Week as one the 25 "Driving Forces of Cyberspace," and recognized at the White House Reception for Internet Pioneers (1998) and the French Ambassador’s medal for assistance to the Washington scientific foreign service corps (1996).