September 22, 2015

Computer Security Resources Center
National Institute for Standards and Technology
Rockville, MD 20850
Via email: nistir8074@nist.gov

Dear Colleagues:

After extensive assessment and review, SC&A is pleased to provide the attached comments on NIST's draft *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (NIST IR 8074).

In summary, we find the draft report to be lacking in specificity regarding the actions taken by the US Government to facilitate standards within the United States or internationally. We also find the recommendations to be too general to enhance cybersecurity in any appreciable manner. NIST should be taking a leadership role in this area, especially in light of its role as the national center of excellence for standards. The recommendations in the report should be more directive and outline what has been working so far and what has not, the role specific government agencies should play and why, and identify specific agencies with responsibilities in the various areas so that progress can be made.

As written, the report suggests that the US Government has not made much progress and cannot unless the White House itself intervenes in leading the standards efforts. We read this as NIST abdicating its responsibilities and delegating them up to the Executive Office of the President. It is NIST's responsibility to coordinate national standards-related programs, and no one other than NIST is capable of addressing the complex standards infrastructure within the United States and internationally. NIST should rely on its own capabilities and utilize the Standards Coordination Office in partnership with the Computer Security Resource Center and the Information Technology Division to address the development of international cybersecurity standards.

The report should be an opportunity to highlight the successes the US Government has made so far working with the private sector and the international community. It should also be an opportunity to outline specific actions that must be taken to further enhance the state of cybersecurity, using international standards as one means to address the ongoing challenges we as a nation have had with a lack of secure computer systems.

Cybersecurity has become a major failing of the United States Government. The topic has been discussed at the senior-most levels of the government for over 20 years with the issuance of Executive Order 13010, the establishment of the President's Commission on Critical Infrastructure Protection, and numerous task forces, tiger teams, NSC staff, etc. over the past two decades. Yet, the Government has been unable to prevent major security breaches that have eroded our confidence in the Government's ability to protect sensitive information. No Cabinet agency has been immune, including with the most recent revelation that the most sensitive personnel data of over 22.5 million citizens held by the Office of Personnel Management has been breached, the Government needs to take a more dedicated and directed approach to cybersecurity. Working to

establish international standards is a start, but from the draft report, one can read that even in this area, not much has been accomplished.

SC&A would be happy to further discuss its comments or assist NIST to address them. Thank you for the opportunity to comment on the draft report.

Very respectfully,

Larry Altenburg
Senior Vice President

Attachment: nistir_8074_vol1_draft_comments_SCA.docx

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	SC&A	Major	Overall	The report does not describe adequately the US Government's activities to develop international standards. While it does a fair job describing the numerous standards organizations within the US and their roles, the report does not describe what government agencies have been involved nor does it outline what actions or efforts they have taken. It also makes a series of recommendations that do not adequately recognize the work done so far, or address the work yet to be done in a coordinated fashion.	The sub-section at line 290 titled "*Interagency and Private Sector Engagement*" of Section "Key Challenges in Cyber Security Standardization" should be pulled out as its own section and expanded to describe specifically what individual government agencies have been involved and the actions and efforts they have taken to address international standardization. The interagency committees should then be highlighted as part of the description of the coordination process used within the US Government, and then finally the challenges and limitations of the current method should be more thoroughly described. More attention should be paid to the work that USG organizations have performed, and if inadequate progress has been made, then the corrective actions and recommendations outlined later in the report can serve to address those gaps.
2	SC&A	Editorial	P2, Line 64	The USG should also exercise care in protection against international organized crime syndicates with financial motivations for breaching the security of critical infrastructures. We suggest using the specific language from the International Strategy for Cyberspace that addresses cyber crime in addition to terrorist and nation state actors.	"Ensuring that international standards meet the cybersecurity interests of the USG including protecting against illicit cyber activities or actions by terrorist groups***, cybercriminals,*** and hostile nation-state actors."
3	SC&A	Major	P8, Line 303	The report indicates the need for US Government-wide coordination at the Executive Office of the President level, but does not describe the efforts made to date nor the limitations experienced by the current governance model. It seems that the report is saying that NIST is unable to address the standards coordination role and that the coordination needs to be escalated to the White House to manage, but the argument as to why is missing.	Describe the specific limitations experienced by the current governance model and why the coordination needs to occur from the EOP rather than by NIST.
4	SC&A	Major	P11, Line 455	The report is calling for "Federal cybersecurity officials with the experience and **bandwidth** to develop and implement a comprehensive set of objectives… [emphasis added]." With the workload of Federal cybersecurity officials what it is, the likelihood of anyone with high levels of experience from any federal agency with availability to participate in the proposed working group is slim at best. The report is proposing the creation of a series of bureaucratic mechanisms and committees that while on the surface would address the challenges identified earlier in the report, would not improve the current situation appreciably.	NIST, specifically, the Information Technology Division (ITD), should take on the role described in the report and use existing mechanisms to address interagency coordination requirements.

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)
5	SC&A	Major	P12, Line 468	This section lacks sufficient actionable details to provide value. Federal agencies should be prioritized and specifically identified for their participation in international standard making and why (e.g., HHS and FDA for medical devices, DOE for SCADA systems)	Outline what key Federal agencies should be involved in international standards development and why. Specifically identify those already participating and those that are not and the SDOs they should be partnered with to ensure appropriate focus from the appropriate agency.
6	SC&A	Major	P12, Line 484	This recommendation is unspecific and not actionable. Clear expectations should be established and assignments made to each particular agency. Further, the recommendation describes a coordination role that should be performed by NIST as the USG's standards body.	Outline the specific actions that NIST as the national standards coordination entity intends to take as well as the actions that should be taken by each specific Federal agency.
7	SC&A	Major	P12, Line 499	This recommendation is unspecific and not actionable. Clear expectations should be established and assignments made to each particular agency. Further, the recommendation describes a role that should be performed by NIST as the USG's standards body.	Outline the specific actions that NIST as the national standards coordination entity intends to take as well as the actions that should be taken by each specific Federal agency.
8	SC&A	Major	P13, Line 512	The recommendation describes a coordination role that should be performed by NIST as the USG's standards body.	Outline the specific actions that NIST as the national standards coordination entity intends to take as well as the actions that should be taken by each specific Federal agency.
9	SC&A	Major	P13, Line 522	Standard training can and should be performed by NIST. This recommendation describes a role that should be performed by NIST/ITD.	Outline the specific actions that NIST as the national standards coordination entity intends to take as well as the actions that should be taken by each specific Federal agency.
10	SC&A	Major	P13, Line 540	This recommendation is unspecific and not actionable. Clear expectations should be established and assignments made to each particular agency. Further, the recommendation describes a role that should be performed by NIST as the USG's standards body.	Outline the specific actions that NIST as the national standards coordination entity intends to take as well as the actions that should be taken by each specific Federal agency.
11	SC&A	Major	P13, line 551	This recommendation is unspecific and not actionable. Clear expectations should be established and assignments made to each particular agency. Further, the recommendation describes a role that should be performed by NIST as the USG's standards body.	Outline the specific actions that NIST as the national standards coordination entity intends to take as well as the actions that should be taken by each specific Federal agency.