Box 883
721 23 Västerås
Sweden

March 12, 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
United States of America

Regarding: "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

To Whom It May Concern,

Where security is a concern, accepting software as fit for use requires deciding whether to accept its contributions to security threats and their mitigation. My colleagues and I have developed a technique for analysing a security standard to determine how well conformance to it supports such a conclusion. This technique could help to ensure that any guidance or standard in the new framework could be relied upon to accomplish its objectives.

The basic premise of our technique is that there is an (implicit or explicit) argument showing how conformance with each clause of a standard supports a series of intermediate security claims and, ultimately, the main claim of acceptability. The essence of the technique is structured, rigorous review and criticism of this argument. Application of this technique to the *Common Criteria for Information Technology Security Evaluation* revealed a number of defects in that standard.

The journal *Information and Software Technology* will soon publish an article describing our technique and some of the defects we found in the *Common Criteria*. Preprint copies and details of our article entitled "Using Argumentation to Evaluate Software Assurance Standards" can be found on the publisher's web site (`http://dx.doi.org/10.1016/j.infsof.2013.02.008`) and on Mälardalen Univeristy's web site (`http://www.mrtc.mdh.se/index.php?choice=publications&id=3268`).

Given our findings, I recommend both the development of an explicit rationale for any guidance or standard being developed or adopted and expert review of this rationale using our technique. I would be happy to answer questions about our technique, our findings regarding the *Common Criteria*, or application of our technique to future guidance or standards.

Kind regards,

Dr Patrick John Graydon
Postdoctoral Research Fellow
Mälardalen Real-Time Research Centre (MRTC)
Mälardalen University
`patrick.graydon@mdh.se`
+46.(0)21 10 14 21

cc: Dr Tim Kelly, University of York, York, UK