From: **HEITZENRATER, CHAD D CIV USAF AFMC AFRL/RIGB**
Date: Mon, Apr 10, 2017 at 1:17 PM
Subject: Comment on NIST Cybersecurity Framework v1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: "HEITZENRATER, CHAD D CIV USAF AFMC AFRL/RIGB"

Cyberframework Authors: I was very excited to see the addition of a metrics section (4.0) in v1.1. I believe this area could be strengthened through the addition of more detailed information regarding what and how things should be measured, to include a stronger discussion of the relationship between leading/lagging --- specifically as it relates to the planning and definition of cybersecurity posture versus the implementation of chosen controls. Current research into areas such as information security economics should prove helpful in defining the planned security approach, complementing risk-based security planning. Likewise, the growing literature on security control effectiveness and interdependency informs dynamic and evolving security efforts. Due in part to this gap, it would currently be difficult to apply the current framework to lower-level implementation details, where risk is less well-defined. Neither set of measurement approaches is well-represented in current standards and guidelines, unfortunately; and therefore is not reflected in the referenced items (although the types of measurements listed above correlate to the notion of "adequate security" used within SP 800-160). Generally speaking, the "Informative Resources" section could be greatly enhanced by the addition of pointers toward maturing academic research.

- Chad

Chad D Heitzenrater
Sr. Computer Scientist, US Air Force Research Laboratory
Information Directorate / Cyber Operations Branch (AFRL/RIGB)