

Dear NIST,

I am submitting my comments concerning two points of the Cybersecurity Framework.

Is the Preliminary Framework:

- 1) presented at the right level of specificity?
- 2) sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?

Specifically, I am referencing page 28, #491, Table 3: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program.

The answer to #1 above is NO as there is no specificity yet at all within the IDESG Policy Committee concerning proposed incentives for Business, and... the Business Environment under Methodology is left blank. It is premature to comment on this framework as the business methodologies have yet to be revealed.

The answer to #2 above is NO as it is not at all clear how the proposed fees for membership in the IDESG will affect individual liberties and abilities for redress. None of the the three categories of Asset Management, Business Environment or Governance have yet been addressed with sufficient specificity. Civil Liberties may well be affected by Agency Agreements involving PII, especially anonymous certificates capable of push notifications to Medical Devices and other Cyber Physical Systems. Interoperability issues have not been sufficiently addressed, nor have technical issues relating to fiber optic redirection and changing information on the fly, retention or verification of real time sensor data, or radio and cell phone interoperability and compatibility issues. Accountability for Cyber Security breaches related to PII and Identity in general have not been articulated.

Sincerely,

Robin L. Ore
IDESG Individual Member