Team 1: *How can Federal Government take advantage of the Trust Architecture?*

- Recommend that the Government engage in an effort with the industry to develop a common framework around a trust architecture that takes into account “Risk, Policy, Assurance, Openness, International Standards” that seeks to enhance the process of building trusted systems (e.g., FISMA).
- The Trust Architecture needs to address the full spectrum of technologies, processes, policies, etc. -- including ‘people components’
- Attempting to reduce the complexity while accommodating legacy systems
- Remediation investment is needed (i.e. guarantee, punishment, effectively dealing with policy violations)
- Solutions need to be applicable Internationally
- Needs to foster innovation

Team 1: Thoughts

- Problem: Do not have a good definition of security.
  - We do not know what the risks are.
  - No framework for comprehensively addressing security exists
- Responding to recurring problems in multiple environments
- Requires: Policy, Policy Implementation, Verifying Implementation
- DOE thoughts: Mandated reporting (CNA, …, FISMA)
- TCG report on Trusted Networks will include:
  - TNC is dealing with some issues but not **POLICY**
  - **Metrics are needed** to measure
- Is the TCG sufficiently structured that you could use as a recommendation to the Federal Government on how to do security?
  - VoIP, video and interactive video complicates this – still need policy
- x.805 (ISO 18028) could be ‘a component’ framework
- Gov’t should understand and operationalize ISO 27001 to help create the method for implementation of security
- Need an assurance plan – open, trustworthy assurance plan – or – fragmentation

TEAM 2: *How can federal policymakers capitalize on trust platforms and solutions?*

- Who are the policymakers? FISMA is implementation, not policy.
- There are various levels of policy makers from OMB down to individual offices and departments. Things like CIO Council tries to do but ends up being consensus and watered down.
- OMB mandates point solutions. What’s needed is a series of point solutions, the security building blocks and the architecture that puts them together. Need to be created hand in hand.
- Lots of different groups and organizations that have opinions about how it should go together – gov’t has different motivators than industry C-level types.

Team 2: Trust for Critical Infrastructures

- Less to do with efficiency and cost savings, more to do with secure information sharing and how do we push the accumulation of intelligence and information out to the edge, in a trusted manner without having to deploy tons of thin clients.
- Look at policymakers motivators at the same time that we build a pilot framework on how this idea could be implemented, show what could be done.
- Critical Infrastructure – There is no SINGLE critical infrastructure.
- DHS has mission to secure the critical infrastructure - but all the CI's are in private sector and so have commercial drivers that need to be considered. E.g., federal policymakers need to consider what drives industry as well as vice versa.
- Public perception of 'what does privacy mean' needs to change.

Team 3: *How can we make trust solutions ubiquitous to globally enhance the state of information technology?*

- First of all – Do we feel that trust is a problem globally?
  - Dimension of the serviceability and the paradigm of the fire extinguisher & the air bags…NRIC Task Force and NGN had varying ideas of how problematic it was.
  - Are the resources the question? Reactive strategy?
- Trust is Pervasive – i.e.. Invisible to the user
- Ubiquitous – How do you implement it globally?

Team 3: What is an example of “trust working?”

- Public switch network
- Elevators
- Sharing information on the internet helped with SARS
- Tech transfer models (NSA?)

Team 3: Features that become ubiquitous?

- What one company does may impact the market
- It is probably standards, regulation
- How do you meet consumer users that do not stay in the technical world…and make the cycle time shorter…
- Communities of users impact…

Team 3: Issues

- A lot of resources are placed in the tactical mode…the fire extinguisher
- Marketing personnel differentiate
- Patents can impact
- There is always the human element…people who will not protect themselves…the grandma and grandpa’s in the voting process for example.

Team 3: Issues

- Will regulation impact the voting process?
- If liability impacted software, then it would change the industry…
- Health care standards
- The market power can make people change
- Need to look at mission critical systems
- In a global economy there are solutions that could jointly be benefited by the joint R&D.

Net: Team 3 – Global Ubiquity

- Paradigm shift – the edge vs. the center!
- Market risk, negative & positive
- Regulation and legislation won’t work by its self
- Hedonic Pricing Model – Charging the customer…Attributes are determined important by the consumer. An example would be SAFETY, thus determining that airbags are an important attribute.