A. Economic and other incentives for enhancing cybersecurity:

- **Current and future challenges:** Our adversaries are coming up with innovative ways to breach our cyber defense. Many of the bad actors do it for monetary profits, apart from the ones who may be state sponsored.

- **Promising and innovative approaches to address those challenges:** In order to build our own knowledge base of finding out and addressing our vulnerabilities, we need to have an insight on the different innovative hacking techniques, used by an array of bad actors, from around the globe.

- **Recommendations:** Build working websites with defense in depth security measures, containing dummy data and transactions. Then invite IT professionals from around the globe (both hackers and crackers) to break into those against monetary rewards. Once they are in this process their action needs to be monitored/audited. The rewards can be stage-based, depending on how far they can advance in the breach process. One can remain anonymous throughout the entire operation and if successful, the specified amount gets deposited in the provided back account. This way we can find out not only about our system vulnerabilities, at the same time, will have valuable insight into the minds and thought processes of a global IT community of cyber experts.

B. Government-private sector coordination and cooperation on cybersecurity:

- **Current and future challenges:** In the current setup, the Government-Private sector coordination and cooperation on cybersecurity has challenges for sharing of technical knowhow and best practices, time sensitive security threats, and actionable intelligence.

- **Promising and innovative approaches to address those challenges:** In order to prepare for tomorrow’s cyber defense, the existing laws and rules needs to be flexible enough which will give more incentives for the public and private sector to communicate to each other.

- **Recommendations:** The Government needs to work with product manufacturers (OEMs) directly, as nobody knows the product better than the manufacturer itself, who owns the source code and other internal technical knowhow. The OEMs can work as the “Technical Partners” to the Government. This is likely to be a win-win situation for both the parties, the OEM getting an opportunity to do partnership with the Government and do stress test on their product capabilities against that volume of live data; and the Government in turn can work directly with the OEM’s product Development team by giving them feedbacks (via product behaviors, bug reports, enhancement requests, etc.). The product can be fine-tuned this way to suit the needs of the Government as well as private sector customers. Also, this way the Government should be able to develop a more “in-house” and “hands-on” knowledge base on cybersecurity, and not solely depend on the Contractor workforce, which seems to be a floating entity, since folks move around from one contractor to another, based on project availability.

C. Federal Governance:

- **Current and future challenges:** At the Federal level, there are challenges for sharing of technical knowhow, best practices and communications, both at an inter-agency and also at an intra-agency level. This results in duplication of cost and resources, leaving the Federal systems vulnerable.

- **Promising and innovative approaches to address those challenges:** In order to prepare for tomorrow’s cyber defense, the existing laws and rules needs to be flexible enough which will give more incentives for the public and private sector to communicate and share information with each other.

- **Recommendations:**
    a. For effective cyber defense, technically savvy leadership (both at the top to mid-level and below) should encourage work force to share information with each other, both at an intra-agency and inter-agency level.
    b. Established technical know-hows and best practices needs to be effectively shared between the agencies, as well as at an intra-agency level
    c. Creation of pool of senior technical SMEs within Agencies (comprising of members from different divisions) who can take mentoring roles and participate in cross team brown bag presentations and knowledge sharing. Before an IT project get implemented within the Agency, the project technical details can be verified by this technical SME Pool. They should be in a position to verify the technical/implementation details from industry experts (both at the Government, as well as Private sector), if needed. That way the Government can ensure that right technology is being implemented, before even the project starts, and not waste precious project $$. The same pool can provide guidance to other Agencies also for similar projects.

D. Technical Advancements:

Other than the above, there are several technical areas which can be explored for effective cybersecurity. Each of them needs considerable write-ups, so just the technologies are mentioned in here –

- Retirement of legacy systems which are difficult to maintain, as well as cost and resource intensive.
- Move towards secured cloud architecture (shared services), particularly for smaller agencies, who cannot afford to maintain an effective in-house IT infrastructure. This way, the agencies can focus better on their business mission, and not spend valuable resources for IT O&Ms.
- Move towards virtualization techniques; towards Software defined Data Centers.
- Software defined networks and Network Function Virtualizations.
- Effective Mobile and Cloud Security best practices.
- Proactive cybersecurity using Data analytics.
- Research Machine learning – to look for deviations from established patterns.