**NIST Big Data Working Group (NBD-WD)**

**NBD-WD-2013/M0013**

**Source: Security and Privacy Subgroup**

**Status: Draft**

**Title: Security and Privacy Subgroup Meeting Agenda for July 10, 2013**

**Author: Arnab Roy (Fujitsu), Nancy Landreville (U. of MD), Akhil Manchanda (GE)**

**Discuss the Security and Privacy Charter**

**Discuss Scope and Requirements**

**Introduction**

This initial list is adapted from the scope of the CSA BDWG charter, organized according to the classification in [1]. Security and Privacy concerns are classified in 4 categories:

1. Infrastructure Security

2. Data Privacy

3. Data Management

4. Integrity and Reactive Security

**Scope**

0. **General**

a. Risk and threat models for big data

1. **Infrastructure Security**

a. Review of technologies and frameworks that have been primarily developed for performance, scalability and availability. (e.g., Apache Hadoop, MPP databases, etc.,)

b. High-availability

i. Security against Denial-of-Service (DoS) attacks.

2. **Data Privacy**

a. Impact of social data revolution on security and privacy of big data implementations.

b. Flexible policy management for accessing and controlling the data

i. For example, language framework for big data policies

c. Data-centric security to protect data no matter where it is stored or accessed in the cloud

i. For example, attribute-based encryption, operation-preserving encryption

d. Big data privacy and governance

i. Data discovery and classification

ii. Data masking technologies: anonymization, rounding, truncation, hashing, obfuscation, differential privacy

iii. Data monitoring

iv. Compliance with regulations such as HIPAA, EU data protection regulations, APEC Cross-Border Privacy Rules (CBPR) requirements, and country-specific regulations

v. Government access to data and freedom of expression concerns

vi. Potentially unintended/unwanted consequences or uses

e. Computing on the encrypted data

i. De-duplication of encrypted data

ii. Searching and reporting on the encrypted data

iii. Fully homomorphic encryption

f. Secure data aggregation

3. **Data Management**

a. Securing data stores

i. Communication protocols

ii. Attack surface reduction

b. Key management, and ownership of data

i. Providing full control of the keys to the data owner

4. **Integrity and Reactive Security**

a. Big data analytics for security intelligence (identifying malicious activity) and situational awareness (understanding the health of the system)

i. Data-driven abuse detection

ii. Large-scale analytics

iii. Streaming data analytics

b. Event detection

c. Security of analytics results

**References**

[1] Cloud Security Alliance Big Data Working Group, “Top 10 Challenges in Big Data Security and Privacy”, 2012.