## Unified Security and Privacy Taxonomy

Use Case: Census

NBD-PWG Security and Privacy SG

January 19, 2016

### 1 Requirements

#### Data Provenance

Data Ownership

Metadata

Cryptographically binding signatures

#### 1.2 Data Privacy

Census individual subject privacy

Privacy of intermediate computations

#### 1.3 System Health

Protection against Denial-of-Service attacks

Protection against Physical Infrastructure attacks

### 2 Concepts

#### 2.1 Data Confidentiality

Individual Subject to Census communication protection

#### 2.2 End Point Input Validation

Mechanisms to ensure input data is authentic

#### 2.3 Privacy Preserving Operations

#### 2.4 Granular Audits

Audits for logging access and use of data

#### 2.5 Forensics

Capability and processes to investigate data breaches

Transaction logs

#### 2.6 Control of Valuable Assets

This may not apply. Does Census monetize data?

#### 2.7 Analytics for Security

Analytics for determining anomalous access to data

### 3 Technologies

#### 3.1 Analytics on logs, cyberphysical events

For forensics, infrastructure security

#### 3.2 Differential Privacy, k-anonymity

Designing access to data for research and privacy preserving information gathering

#### 3.3 Digital Rights Management

This may not apply

#### 3.4 Access Control Model

##### 3.4.1 Identity

Identity and roles management for accessing data

Staff, researcher, management and so on

##### 3.4.2 Authentication

Authentication of identities accessing data

##### 3.4.3 Authorization

Processes to endow data access privileges

May be based on institutional processes and contract with research organizations

#### 3.5 Key Management

Key management for digital signatures, data encryption, access control

#### 3.6 Authenticated Computations on Data

Cryptographically authenticated computing on data – active research field – deployment may be nascent at this point

Can be used to delegate computations to third parties and make sure that the results computed are legitimate

Relevant reference: Gennaro, Gentry and Parno, “Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers”, CRYPTO 2010

#### 3.7 Computing on Encrypted Data

Can be used to outsource computations to third parties, without giving them decryption keys

Fully homomorphic encryption: First construction by Gentry, 2009

Functional Encryption: Concepts formalized by Boneh, Sahai and Waters