For the Government Survey, here is a description and examples of each challenge area:

- **Analysis (i.e., large scale, logs, correlation, timelines, etc.)**
  Cloud forensic analysis includes topics such as the capture of log and other metadata and their meaningful attribution to cause; unification of log formats; forensic time line analysis of log data; correlation of information across and within cloud providers, content, and metadata; synchronization between and determination of precision and accuracy of time stamps; etc. where one or more elements under investigation resided in, or transited a cloud.

- **First responders (i.e., storage and systems controlled by cloud provider, volatile data preservation, data access, live systems, etc.)**
  First responder issues in cloud forensics include topics such as the ability to image media and isolate a moving data target; confidence, competence, and trustworthiness of the cloud provider to act as a first responder; challenges in response time due to location uncertainty; real-time, live access to data on international cloud services; etc.

- **Legal (i.e., jurisdiction, laws, service level agreements, contracts, etc.)**
  Legal issues in cloud forensics include topics such as identifying and addressing issues of jurisdictions for legal access to data; limited investigative powers; channels for international communication and cooperation dealing with an investigation; data acquisition that relies on the cooperation of cloud providers; missing terms in contracts and service level agreements; etc.

- **Architecture (i.e. topology, diversity, proprietary information, etc.)**
  Architecture issues in cloud forensics include topics such as variability in cloud architectures between providers; decreased access to forensic data that varies between the cloud models that have been implemented; accessing the data of one tenant without breaching the confidentiality of other tenants; etc.

- **Data collection (i.e., data location, data recovery, data segregation in multi-tenancy environment, data integrity, imaging, etc.)**
  Cloud forensics data collection includes topics such as collecting data while the suspect system is still running and while data are likely to be changing; data collection and preservation from virtual machines; the lack of knowledge about ownership, custody or location of data in a multi-tenancy and distributed environment; etc.

- **Standards (i.e., ISO, chain of custody, cloud regulations, no single process, etc.)**
  Standards in cloud forensics include topics such as lack of standard nomenclature/ontology for cloud forensic terms as well as for reporting results; few standard operating procedures, practices, and tools; lack of interoperability among cloud providers; etc.
• **Anti-forensics (i.e., malware, data hiding, modus operandi, etc.)**
  Anti-forensics are a set of techniques used as countermeasures to forensic analysis. The term includes topics such as the use of malware, data hiding, or other techniques to compromise the integrity of evidence; etc.

• **Training (i.e., legal, first responders, forensics examiner, etc.)**
  Training in cloud forensics includes topics such as attempts to use digital forensic training materials that are not applicable to cloud forensics; the lack of training and forensic expertise for cloud environments; the lack of familiarity with virtualization by investigators and evidence collectors; etc.

• **Role Management (i.e., data owners, attribution, identity, users, etc.)**
  Role management in cloud forensics includes topics such as unique identification of the owner of an account; the decoupling between cloud user credentials and physical users; the ability to create entire fictitious identities online; determining which user owns certain data; determining which user has access rights to certain computing functions; etc.

• **Other**
  This category covers other cloud computing areas of challenges. Please provide a specific description, and please focus only on cloud (as opposed to non-cloud) environments.