KICKOFF MEETING AGENDA

1. **Introduction of the new NIST Cloud Computing Forensic Science Public Working Group and its purpose.** (Marty Herman)
   - Introduce Michaela Iorga and Eric Simmon as co-chairs.
   - Emphasis on
     - Develop a common framework to support cloud forensic science
     - Gathering input from stakeholders on issues and challenges dealing with cloud forensic science
     - Developing R&D and standards-development plans based on the challenges
     - Gathering input on use cases and goals
     - Developing taxonomy and requirements
     - Strawman definition of “cloud computing forensic science”

2. **Present goal decomposition – how to use goals and use cases to develop requirements for cloud forensic science** (E. Simmon)

3. **Present the existing NIST CC Reference Architecture and Taxonomy; present the existing NIST CC Security Reference Architecture** (M. Iorga)

4. **Facilitate discussion on how to proceed from here** (Michaela & Eric):
   - Gathering input from participants
   - Using the Twiki
   - Gathering goals and use cases
   - How to develop a CC forensic science common framework, leveraging the RA and FRA and any other relevant CC forensics architectures
Strawman Definition for “Cloud Computing Forensic Science”

Many experts consider forensic science to be the application of a broad spectrum of sciences and technologies to the investigation and establishment of facts of interest in relation to criminal or civil law. However, the resulting techniques may be used for other purposes outside the scope of law to reconstruct an event that has occurred. Digital forensic science encompasses the techniques for recovery, analysis and investigation of information found in digital devices.

Cloud computing forensic science is defined as follows: After an event has occurred in a cloud computing system, cloud computing forensic science provides scientific-based methodologies for reconstructing the event based on the identification, collection, examination, analysis, reporting of digital data and preservation of the digital evidence.

Note1: Examples of such events include criminal activities, computer security incidents, internal policy violations, operational problems, and accidental system damage.

Note2: The cloud computing system is defined in NIST SP 800-14, “The NIST Definition of Cloud Computing.” Suggest we use a different reference.
PROPOSED TOPICS:

1. Vocabulary - put team together to develop a CCFS taxonomy/vocabulary

2. Goals analysis - put team together to update goal decomposition and develop supporting use cases

BI-WEEKLY MEETINGS:

Day: Thursdays
Time: 1:00 PM or 2:00 PM EST,
Starting: Nov 29, 2012