This outline is intended to identify the policy and other requirements and preferences of the multiple stakeholders involved in any attribution system so as to drive subsequent technical developments of GENI attribution capabilities. 'Requirements' reflect the needs of a comprehensive attribution system.

The goal of this outline is to organize possible attribution features that may prove useful. All will be mentioned in the final report, but that report will focus on those attributes most relevant to the GENI project.

I. The Problem of Attribution

a. The technical literature discusses 'attribution' in many forms, but usually in isolation from the non-technical world, or focusing on specific real-world problems (e.g., attributing the source of packet attacks) for which the proposed mechanism provides (sometimes limited) solutions
b. Attribution must be examined from the viewpoint of multiple stakeholders

II. Definition and Purpose of Attribution

a. Dictionary definition
b. Specific to technical cyber security needs
c. Specific to legal needs, such as use as evidence, so that attribution characteristics can be merged with cyber security data to be used as evidence in court
d. We define 'attribution' as the association of data (called a *characteristic*) with an entity (person, process, file, other data).
e. Goal of attribution is to show that the characteristic associated with an entity has a particular value, or one of a particular set of values.
f. Purpose for using attribution is generally that of accountability
g. Our concept of attribution involves an expanded definition that includes interests other than that of the recipient; it encompasses the interests of senders, network perspectives, and other (possibly secondary) requirements.

(see text for Sections I, II)

III. Requirement (1): Set of Actors

a. Need to model nine different entities that have an interest in attribution:
    i. The sender of the message;
    ii. The organization associated with the sender;
    iii. The governments of the country of the sender
    iv. The ISP's over which the message transits
    v. The network backbone providers over whose backbones the message transits;
    vi. The governments of any intermediate nations through which the message transits;
    vii. The governments of the country of the recipient
    viii. The organization associated with the recipient
    ix. The recipient

b. Is this important to GENI ?(TBD)
c. How is this requirement met? (TBD)

IV. Discussion: What is Being Attributed

a. This is shaped by three considerations:
    i. Interests and capabilities of the different parties(actors) that define the characteristics of interest for attribution
        1. Desired sufficiency of the attribution
        2. Nature of the actions for which attribution is desired
        3. Intended purpose of the attribution
    ii. Level of certainty associated with showing that the characteristic associated with an entity has a particular value, or one of a particular set of values
    iii. The possible gap between the level of attribution achieved and the level of attribution desired
b. The Attribute Vector
    i. Paired set of elements: characteristics, and values (or values which are requested)
    ii. Attribution attributes defined and accepted (in the case of cooperating parties)
c. Attribute Assurance
    i. Confidence that the values of characteristics are correct.
    ii. NB: 'Acceptance' of an attribute vector is thus a multi-attribute decision choice. For discussion: should this be part of somebody's future work?

V. Actor's Attribution Policy Requirements: Defining what Individual (independent) actors 'want':

a. Senders and receivers may require different attribution policies
    i. Motivating examples: A government web site might require attribution to the user level, but be willing to negotiate down to just an IP address should the user prefer not to provide personal identify. Conversely, a dissident web site needs to advertise its policy of not accepting any forms of attribution before a visitor accidentally provides some (correct) attribution information. (see Policy Negotiation below)
b. Actors define 'acceptable' attribution and an 'acceptable' level of attribute assurance, or determine that no such level is possible under the extant circumstances.
c. Requirement (2): Policy requirements of senders and receivers
    i. Recipients may want :
        a. Perfect non-attribution
        b. Perfect attribution
        c. Perfect selective attribution
        d. Sender non-attribution
        e. Recipient non-attribution
        f. Unconcern

ii. Senders may want:
    a. Perfect non-attribution
    b. False attribution
    c. Randomized false attribution
    d. Imperfect attribution
iii. Examples
    a. Sender: false attribution; recipient: perfect attribution (your gov't intelligence agent visiting a terrorist web site)
    b. Redo the example in a.i. of this section showing the requirements met or desired

d. Requirement (3): Capturing Interests of ISPs and backbones
i. Business interests – ISPs may want to provide attribution services only if they are profitable and the ISP is unlikely to be sued
ii. Balance of profitability and liability
iii. Included in liability are cultural and legal constraints

e. Requirement (4): Capturing Requirements/Interests of other parties

f. Implications for GENI
i. Are these important to GENI? (TBD)
ii. How are these met? (TBD)

VI. Requirement (5) for Special Case of Cooperating Senders and Receivers

a. Attribution attributes carefully defined and accepted by all parties
b. Agreed upon mechanism for negotiation among all parties
c. Backbones and Intermediate nodes have no generic incentive for cooperation: thus cooperating senders and receivers have to specify some attributes of the network path (policy based routing)
d. Implications for GENI
    i. Are these requirements important to GENI? (TBD)
    ii. How are these met? (TBD)

VII. Special Desired Characteristics of Attribution Assurance:

a. **Requirement (6)** :(Ideally) metrics or means of senders/recipients (or whatever nodes need this – to be called *trust client nodes*) to assess trust in the accuracy and security of the communication of the attribution characteristics.
    i. Discussion: Metrics might be placed in backbones and intermediate nodes. Alternatively, perhaps 'metrics' is the wrong way of thinking about information provided by intermediate notes. Perhaps "trust" is made up of several measures, and that the intermediate nodes record data that the trust client nodes get the data. In this formulation, each trust client node may have their own idea of how to compute trust, and should not be constrained to using a single trust metric (or fixed set of trust metrics)

ii. Discussion (2): Perhaps specification of data recorded for used by each trust client node is in itself part of the policy negotiation.
iii. **Requirement (7)**: Policy based path routing necessary to ensure the paths provided the 'appropriate' support for attribution

b. **Requirement (8): defining level of assurance of values**
c. Implications for GENI
    i. Are these requirements important to GENI? (TBD)
    ii. How are these met?

VIII. Requirements for General Case of Non-cooperating Senders and Receivers

a. Motivation: political dissidents in repressive regimes:
    i. sender (probably) will not want attribution
    ii. recipients (international community at large?) will not want senders to have their messages attributed to them
    iii. governments/organizations want attribution of sender (for repressive political reasons)
b. **Requirement (9):** Addressing challenge that without the cooperation of sending governments and organizations, creating a policy based routing system will depend on:
    i. Technical specifications that establishes the policy based trust network
        1. **Requirement (10):** Defining the extent to which the trust network can in fact be trusted
c. Challenge: multiple choices exist in this scenario: how to sort out which are 'best'?
    i. Politically dissident senders may choose not use network
    ii. Recipients may be less trusting of traffic without sender attribution
    iii. Intermediate nodes and backbones may cooperate with the sending governments/organizations – implications for reliability of policy based trust network?
d. Implications for GENI
    i. Are these requirements important to GENI? (TBD)
    ii. How are these met? (TBD)

IX. Requirements: Attribution Vector

a. Requirement (11): Defining Elements of the Attribution vector
    i. Attribution vector is a sequence of pairs
        1. 1st element: characteristic for which value is either present or desired
        2. 2nd element: value of characteristic, or indication that characteristic is either requested or not available
    ii. Suggested elements:
        1. Origin of source
            a. Defining 'source': user, IP address, organization, geographic region? (see discussion of source below)

2. Time
3. Route
4. How message was protected (e.g., encryption or access control bits)
5. Where geographically did the message travel

b. **Requirement (12): defining level of assurance of values (see above)**
c. **Requirement (13): specifying origination of attribution**
   i. Motivation: while typically one thinks of attribution as relating a packet back to an originating machine, that may be insufficient, or even misleading and meaningless (e.g., attribution back to a botnet).
   ii. Motivation: Desired attribution may be back to an individual or to a class of individuals. For instance, attribution that the sender is a medical doctor, or is over the age of 21, may be sufficient, without needing any further individual attribution.
d. **Requirement (14): Defining to whom the attribution information is reported**
   i. Motivation: Attribution is traditionally thought of as the ability to determine, based on the interest of the recipient, where the message came from. But what if one's spouse is acceptable attribution recipient, but one's employer is not?
   ii. Attribution information can in general be reported to:
      1. Recipient
      2. Some central authority
      3. Other intermediate nodes, who find it of value to know what traffic is occurring between two different locations
e. **Possible Requirement (15)**: Defining the characteristic of why the message was sent
   i. Dealing with this remains an open research question
f. Are these requirements needed for GENI? TBD
g. How are these met? TBD

X. Policy Negotiation Structure

a. Motivation: With nine different classes of actors potentially involved in the attribution, typically a policy negotiation will be required in order to establish an agreed upon attribution vector.
b. Definition: Such as agreed upon attribution vector is a *policy contract*
c. *Overarching issue:* What is the infrastructure (technical, policy, organizational, social) needed to support an effective policy negotiating system?
d. **Requirement (16) (KEY REQUIREMENT):** A policy contract negotiation system must be workable and agreeable to all parties
   i. **Requirement (16.1):** a common nomenclature of attribution vectors (policy contract elements)
      1. Desired in policy contract: length of the agreement; specified trust levels among network parties (particularly ISP's and backbones); penalties for non-performance

ii. **Requirement (16.2):** system for communicating and negotiating the policy contract among the different parties
    1. Desired: should be transparent, low cost, made routine and commonly accepted
iii. **Requirement (16.3):** ability by each party to specify and communicate desired attribution states and levels of assurance
iv. **Requirement (16.4):** a verification system for ensuring that contracts are performed
    1. Issue: how to ensure that the entire policy contract negotiation system is enforceable
    2. Verification mechanism needs to provide consequences for following or failing to follow negotiated contracts.
v. Issue: Policy negotiations themselves cannot violate existing policies
    1. Motivating example: A sender may already have as its policy that its identity never be attributable.
    2. Possible approach: provide a trusted storage mechanism for existing policies which specify the framework for further negotiations or identifies specific types of policy negotiations that may take place between either wholly or partially anonymous parties.
vi. Issue: Avoiding unwanted accidental outcomes:
    1. Motivation: a dissident web site needs to block, and advertise, its policy of not accepting any forms of attribution before a prospective user accidentally provides it.
    2. Further discussion: a parallel real world example is the 'negotiation' that takes place between a recipient with a telephone blocking calls that suppress caller ID, and a caller (sender) whose telephone does not transmit caller ID. This either requires some other mechanism to initiate communication, or simply the sender determining that communication is not possible. Under what circumstances is this 'acceptable'?

e. **Requirement (17):** There needs to be a trust network enabling actors to trust that other actors, and the network, will honor their commitments as negotiated in the policy contract.
    i. Signers of a policy contract (NB – how is a policy contract signed?) must have some measure of trust in other actors to provide *acceptably accurate* attribute values.
        1. Trust system might be tied to the verification system (see above)
        2. Function much as a reputation system would?

f. **Requirement (18):** Policy based routing mechanism is needed to ensure that messages traverse networks and midpoints with 'appropriate' attribution mechanisms and levels of trust.
    i. Motivation: the path that the message takes affects both the values in the attribute vector and the level of assurance of that vector (including the values)
        1. Unless:
            a. Actors do not care whether the attribution changes in transit (NB: Is this ever the case?)
            b. Or intermediate nodes cannot alter the attribute vector and do not add any attribute data of their own.

XI. Governance Issues

a. Ensuring governance is dynamic, reflects the changing needs of users, administrative domains, and other interested parties.
b. The 'Superuser' or 'Administrator' in which one (or more?) privileged users can override normal user controls.
    i. Purpose: traditionally this mechanism is used to provide an escape to correct severe problems or failures
    ii. Issue: defining the role of central authorities for overriding the policy-based trust network under defined circumstances
        1. For technical reasons? For policy reasons?
        2. Multi-jurisdictional roles?

    Key question: should such an entity exist? What happens if not?
    iii. Issue: multiple central authorities? NB: If multiple central authorities are involved in creating (or assuring) an attribution vector, what is the basis for cooperation among them? (e.g., will this require each authority has only limited access to attribution vectors of other authorities?)
c. Extent of adoption of common protocols to implement the policy negotiation system.
    i. Is attribution ubiquitous?
    ii. A single protocol or inter-operable protocols?
d. What constitutes 'adequate' attribution, and who decides?
e. Revocation – when can attribution be undone or repudiated?
    i. In a centralized system, a central authority could direct all networks (specifically intermediate nodes) to discard all attribution information.
f. Selective access to attribute vectors: defining circumstances and mechanisms for this (see above).

XII. Governance Issues: Conflict Resolution

a. Motivation: Negotiation system and supporting infrastructure must handle conflicts and ambiguities appropriately. For example, attribution may be desirable for crimes and cyber attacks, and undesirable for political speech and whistleblowers.
b. Actors may (will) have different, conflicting goals and values.

i. More than a technical problem: e.g., delves into political and cultural aspects of attribution, e.g., our culture assumes that ability to visit a dissident web site is good but governments of some countries would strongly disagree with this belief.

XIII. Requirement(19) for False Attribution

- **a.** Under some circumstances (e.g., national defense, counter-intelligence) there is a requirement for false attribution.
  - **i.** Under what circumstances should this capability be available?
  - **ii.** How do we constrain its use?
- **b.** If not always available, who should determine what circumstances warrant its use? Who decides whether those circumstances are met?

XIV. Governance Issue: Economics

- **a.** Intuition is that the economic flows from a full attribution system will be considerable, and that a variety of business models can emerge variously trading off trust, traffic volume, cost, and even side payments from other parties.
- **b.** Policy choices may shape the ultimate network economics
- **c.** Issue: What is the 'path' for developing an attribution system, and who decides?
- **d.** Who pays? How will needed multilateral capabilities be built? These include:
  - **i.** A common multilateral policy framework to formalize cooperation, definitions, and collaborations necessary for attribution across administrative, jurisdictional, and national boundaries
  - **ii.** Technical cooperation to fill important current gaps, e.g., research, recommending (specifying for requirements?) best attribution techniques, providing support
  - **iii.** Negotiating structures for all nine sets of parties involved with defined terms for levels of attribution and non-attribution to be associated with each message
  - **iv.** Policy based trusted network routing across backbones/nodes.

XV. Other Issues

a. A return receipt acknowledging message received/read: authentication?