Responding to Inter-organizational LLR Requests in the GENI Federation

Document Name: Responding to Inter-organizational Legal, Law Enforcement & Regulatory Requests in the GENI Federation
Document Type: MOU
Version: 0.3.0 (Draft)
Date: Nov. 1, 2011

Executive Summary

At first glance, it may appear that the GENI federation and the GENI Oversight Group have no legal responsibilities of their own since "GENI" owns virtually no infrastructure and experimenters are ultimately responsible for the actions of their individual experiments. While both statements are true, there is a subtlety here as (1) lawyers, law enforcement and regulatory agencies (LLR) do not know this, and (2) no one party necessarily has all the information to address inquiries from these entities. Therefore, collaboration will be necessary to resolve some LLR issues and the need for a plan to handle such requests is clear.

This document begins by further motivating this need with several scenarios or use cases, some based on previous experience in other federations and testbeds. These scenarios also drive the need for proactive measures, such as, having a simple mechanism to reach slice owners and heading off future DMCA requests which could discourage campus participation in GENI. Finally, it becomes clear that someone is needed to fulfill a facilitator role to help route LLR requests to the appropriate parties when a single institution is unable to address the request it receives entirely on its own.

We are calling this facilitator the GENI LLR Representative, and we define the responsibilities of this role in this document. It is important to realize that this person is a facilitator, and not an authority who can dictate action to various parties. Their job is to route LLR request to their proper place, or at least always get them one step closer. For example, they may help to identify a slice corresponding to some undesired behavior, or put a requesting party in contact with a slice owner about the behavior of their slice. However, it is the slice owner and corresponding project leader who are ultimately responsible for the behavior of a slice, and aggregate authorities are to decide themselves according to institutional policy and local laws how to respond to requests that are routed to them.

We further define a set of capabilities/responsibilities and procedures for handling anticipated types of requests. By capabilities, we are speaking of information that different parties should know, or questions they should be able to answer. By responsibilities, we are defining new ones only for the role of an official GENI facilitator to assist with these types of requests. Responsibilities on other parties (e.g., aggregate authorities, slice owners, project leaders and campuses) referenced in this plan must be established in other agreements if they are to be binding. This document itself is not a legal agreement, but defines a problem, a new role and a set of processes to resolve LLR issues both anticipated and not.

These capabilities are important to note here while the control framework architecture is not yet set in stone. If developers are not aware of these needs, a framework could evolve that does not support even the high-level process and procedures defined at the end of this plan. The ability to execute these procedures is critical if members of the GENI federation are to effectively handle LLR requests whose failure to be addressed would impair adoption of GENI at future institutions.

Representative Scenarios

To help understand potential LLR requests that the GENI federation may need to prepare for, we illustrate issues that may come up with the following four scenarios. These are in no way meant to be exhaustive, and with experience operating GENI new issues may arise and others may become less relevant. These scenarios serve as a thought experiment to prepare for requests that could otherwise derail GENI, for example, by discouraging campus adoption.

DMCA Takedowns

A GENI resource at a university may be thought to have downloaded copywritten media from a torrent site, in which case that University's IT department will need some way to associate a user (or set of users) with a GENI resource at a particular time. The university may come to GENI if they don't know who is responsible for the host, again requiring the GENI representative to be able to redirect them to the appropriate party.

However, even if they do find the aggregate operator on their campus, that does not mean that the aggregate operator can answer the question. They may only know the slice responsible and nothing except attributes of the slice owner or experimenters. What they will need to be able to determine is the project leader responsible for the slice and how to redirect the campus IT or legal department to that person who could answer questions about the behavior of their slice. This means that the aggregate operator may need to work with the GENI Clearinghouse or some other GENI slice authority to resolve such an issue. Regardless, that other entity must be able to map slices to an actual person responsible for the slice, or at least put a LLR party in contact with the slice owner or associated project leader.

Contraband Downloads

A federal agent could contact the GENI Oversight Group (GOG), the GPO, the GMOC or another entity that *they believe* to have governance or operational responsibilities for GENI. This could be in regards to an IP address and time recorded for a download of child pornography, classified documents or some other contraband materials. While it seems likely they would go to the institution hosting the resource first (e.g., the Aggregate Authority's [AA's] campus CIO), they could first be directed to GENI for any number of reasons.

This agent would need to know if this is indeed a GENI resource, and who is responsible for the host/device. If the GENI LLR representative does not know, they must at least be able to route this agent to a specific Aggregate Authority or other party who could answer the agent's questions.

Seized System

A law enforcement agency may seize a system in the course of an investigation and learn that it is or hosts a GENI resource. In most cases, the institution at which the host was seized would be able to answer their questions, but university IT departments often know little about systems used for research projects. Therefore, an agency may inquire for more information from someone they perceive to be a GENI representative.

This GENI LLR representative should be able to determine if the resource is a part of GENI, or at least be able to route the agency to someone who could answer that question. For example, if the machine is seized from a particular university, they may redirect the agent to the GENI aggregate operators at that institution where it was seized. These operators should be able to say who is responsible for the machine and/or the services/applications hosted on the machine if they do determine it is a GENI resource. Furthermore, they should be able to redirect the request to the project leader of whatever experiments are being run on the machine, or at least to someone who could make that determination, i.e. the Clearinghouse or appropriate slice authority.

Criminal Defense

In criminal trials of various cyber crimes, a common defense tactic is for the defendant to claim that “hackers” or some other malicious process downloaded the illegal material or launched an attack. It is conceivable that an opt-in user who has installed "GENI software" on their computer could try to blame GENI, in which case lawyers, through legal discovery, would try to get all the information they could on the relevant GENI software.

In all likelihood, they would come to some high-level representative of GENI with their questions. The GENI LLR representative would need to know to whom to redirect the lawyer's team to get more specific answers. Therefore, any official GENI representative would need to know about aggregates or experiments installing software on opt-in user devices and be able to provide the requesting party with detailed technical descriptions of the functions and capabilities of that software. This could be as simple as providing the requesting party with a prepared document written specifically for this purpose.

Capabilities & Responsibilities of each Party

A common thread running through all of these examples is that if GENI is to be prepared as a federation to adequately address legal and regulatory issues, a *GENI LLR Representative* must be appointed and have the knowledge to properly route requests from LLR entities, or from GENI host providers/researchers who have received requests from LLR agents which they cannot fully answer. This is the person who will be the public face to the "LLR world", and it is to this person that all LLR requests to speak to a "GENI official" should be routed. They are a facilitator, and not an authority, though. The role of this person is a technical expeditor, helping to answer questions and get the right parties in touch. They do not have the authority to tell AAs what to do or to shut down slices themselves, while acting in this role.

It is unclear where this role should reside at this time, and ultimately it will be up to GENI Oversight Group in the future to decide. If a CSO role is ever created for GENI, then this may be one additional hat that person wears. In the interim, the GPO should appoint someone in the community familiar with these agreements. **Regardless, all parties involved in GENI and campuses with GENI aggregates should be aware of this role, and it must be easy for outsiders to determine who to contact for LLR requests.**

The GENI LLR representative should:

- Be able to direct an LLR agent to the AA(s) responsible for resources at a particular organization and be able to answer whether or not a given organization even hosts a GENI aggregate;
- Be aware of any aggregates or experiments that install software on opt-in user devices, and be able to redirect LLR requests about such software to the appropriate aggregate operator or experimenter familiar with its development;
- Be able to redirect an LLR request about a particular piece of GENI infrastructure software to the appropriate technical team that could answer further questions;
- Be able to determine the real world creator of a given slice, be able to put an entity in communication with a slice owner, or be able to redirect an LLR request to someone else that could accomplish the aforementioned goals; and
- Be able to determine if a given IP address with an associated timestamp corresponds to a GENI resource, or be able to redirect an LLR request to the AAs at the institution which could make that determination.

Aggregate Authorities or Aggregate Operators should:

- Be able to tell if a given IP address with an associated timestamp corresponds to one of their GENI resources;
- Be able to determine what GENI slices are running on their components;

- Make known to the GENI LLR Representative any software that they may install on opt-in user hardware; and
- Be able to confirm if a seized piece of hardware is from their aggregate;

The GENI Clearinghouse should:

- Be able to map slices to real world slice owners and project leaders or at least put a requestor in contact with both, perhaps through the assistance of the issuing slice authority. If delegating authentication to an identity provicer, they should be able to reroute such requests to the appropriate identity provider who could authoritatively map a project leader to a real person.

Project Leader or Slice Creator must:

- Make the GENI LLR Representative aware of any software which they install on opt-in user hardware;
- Take responsibility for the actions of their experiments; and
- Use their own identity when creating a project or slice with correct contact information if applicable.

Being Proactive

A realization, which should be clear from the lists above, is that establishing good communication channels between the GMOC, Aggregate Authorities, Clearinghouse and campus IT departments will be critical. In fact, this has been noted in the Emergency Stop Plans, the Aggregate Provider Agreement, and in this document where we have emphasized that all parties must be able to identify the *GENI LLR Representative* and that the person filling this role should be able to reroute requests to the appropriate parties.

Of significant importance to GENI's success is the relationship with campuses hosting resources. They are dedicating significant space and bandwidth to the various aggregates and asking for little if anything in return. If their IT or Legal Departments have to spend significant time with LLR requests related to GENI resources, they will have little incentive to keep those systems online. PlanetLab has learned about the importance of this relationship, and they have been quite proactive in protecting it in a way that GENI should consider as well.

Of all the scenarios described herein, experiences from PlanetLab would suggest dealing with DMCA takedowns is inevitable. The algorithms to detect alleged violations are very coarse and have high false-positive rates. Several experiments, especially with P2P protocols and file-sharing protocols, have falsely triggered such letters. In fact, PlanetLab has gone so far as to get one of the organizations that sends out these letters to whitelist PlanetLab hosts. We recommend a similar approach for GENI as well.

A complete list of IPs of GENI resources would be very useful and allow the GENI federation to be more proactive with DMCA takedown notices. These notices are likely to go first to campus personnel who know little or nothing about the hosts in question, and they are likely to tire of them quickly if these letters become a common occurrence. Therefore, official GENI Aggregate Authorities agree to provide the GMOC with IP blocks that they will be using for the public interfaces of any of their GENI components and slivers so that (1) the GENI LLR can more quickly route potential requests, and (2) GENI can try to get its experiments whitelisted from such DMCA bots. While the diversity and scale of GENI may not make this 100% achievable, the 90% case could be addressed to the benefit of many.

Additionally, it should be apparent that many requests will ultimately land in the hands of the experimenters or slice owners. This is because GENI places the responsibility for the behavior of a slice in the hands of the experimenter first, slice owner second and project leader finally since they delegate the ability to create slices. This ultimate responsibility on the project leader is important because (1) the actual experimenter at a given time might not be identifiable and (2) each slice needs a "grown-up" responsible for it, like a PI. **Therefore, we strongly recommend email aliases be created for each slice.** So an address like *slice-367@geni.net* would go to the person who created slice number 367. This one technical capability has the potential to shortcut many investigations by putting the requestor in direct contact with the slice owner more quickly and in a way that does not consume the time of the Clearinghouse operators.

Procedures

The primary job of the GENI LLR Representative is as a facilitator, putting the right people in contact to handle LLR requests according to the policies and procedures of their home institutions. It is important to recognize that this is a best effort service, with no guarantees because different federation members have different policies and procedures and may even have different technical capabilities. If an organization crucial to resolving an LLR request is a university that only stores logs for 30 days, then a request may hit a dead end. Alternatively, the privacy policies at another campus may prevent them from cooperating, even though the GENI LLR representative did do their part and successfully put a law enforcement agent in contact with the party who has the information sought. Lastly, it must be remembered that identity providers may not checking government IDs for account creation; so there is always uncertainty in the real world identity of an experimenter. In all these cases, the GENI LLR is still capable of performing their duty and meeting GENI's responsibility of trying to route these requests to experimenters or those hosting the devices under question.

While it is impossible to anticipate all possible scenarios, we can develop a generic framework for handling LLR requests. Rather than create specific flowcharts for all the possible permutations of request flows, we specify a few simple rules that will allow each party to get requests to their proper next hop. In this way, what we specify here is more like routing tables than source-based routing. In each section below, we describe what a particular party should do with a particular type of request, of course recognizing that they are bound by their institutions rules and regulations.

Project Leader or Slice Creator

If an LLR request ends up going to a slice creator or project leader, it is most likely about the behavior of their slice(s). The slice owner or project leader should answer all questions to the best of their ability as they are responsible for the slice. Experimenters that are performing illicit activities

cannot expect that they will continue to be allowed access to GENI resources. If the experiment in question is run by a delegate of theirs, then they should refer the request to that delegate for more information if necessary.

If the slice creator or project leader does not know what to do with a request or believes it has come to them in error, then they should contact the GENI LLR Representative who will help to resolve the issue.

Campus IT

Campuses are likely to receive two types of requests: either to identify a real world person associated with an GENI user ID (if they are an identity provider), or a direct request from an LLR agent about a host in their IP space that may be a GENI resource.

In the first case, the request for identifying the owner of a slice was likely forwarded from the Clearinghouse (perhaps another slice authority or identity portal). This may have been forwarded with the help or knowledge of the GENI LLR Representative. In this case, it is presumed that the slice authority (perhaps at the Clearinghouse) could not directly answer the question themselves, perhaps because they only know certain attributes of the users (e.g., a student from University X). The campus should communicate directly with the LLR agent about this request following the policies in place at their institution. (Note: this whole process could be carried out with any identity portal or identity provider and is not specific to campuses acting through InCommon)

A campus IT representative may also directly receive a request from an LLR agent about a host in their IP space. If it is known to be a GENI resource, they should know to contact the GENI aggregate operators or AAs on their campus. AAs are expected to make their campus IT departments aware of GENI aggregates they host on campus, and therefore they should know who to contact. If somehow a campus IT department knows a resource is for GENI or GENI-enabled, but does not know who the aggregate operator or AA is, they can contact the GENI LLR Representative who will provide them with that information.

Campuses should handle such LLR requests according to their policies or procedures, but if they require extra information (that cannot be answered internally) about either GENI in general or the specific slices and experiments running on a resource, they should request the assistance of the GENI LLR Representative who can put them in contact with more knowledgeable parties.

Clearinghouse or Slice Authorities

The Clearinghouse is unlikely to directly receive any LLR requests except possibly in regards to their own machines if compromised. However, an AA or the GENI LLR Representative could redirect an LLR agent to them to identify a slice owner regarding the behavior of a specific experiment. The Clearinghouse should follow its host organization's policies for handling such requests. If they do not have the information to map a slice creator to a real person, they should redirect the LLR requestor to the party to whom they delegated that authentication, such as an InCommon campus identity provider or another identity portal. Alternatively, it may be sufficient just to give the requesting agent contact info that allows them to directly contact the slice owner, such as a per slice email address.

Aggregate Authorities / Aggregate Operators

AAs are likely to receive a request either from their organization's IT departments, or ones forwarded from the GENI LLR Representative. In the first case, it is completely an internal matter to the hosting organization or campus. If in the course of the investigation they need information that they cannot answer, (e.g. what is an experiment doing or who owns an experiment running on their aggregate), they may enlist the help of the GENI LLR Representative or directly refer the requesting LLR agent to the experiment owner or the clearinghouse who may be able to identify the owner.

An AA or aggregate operator may receive a referral from the GENI LLR Representative if somehow an LLR request did not come directly to their hosting institution first, but more likely they would receive a question from a GENI LLR Representative about whether or not an IP address at a given time is part of their aggregate, meaning a resource under their control or a sliver on a resource under their control. They may not have the capability to rule out whether or not an IP address is associated with one of their opt-in users, and agreements with those users or their own institution's policies may prevent them from identifying opt-in users. If this is the case, it should be clearly stated.

Of course, any referral from the GENI LLR Representative could lead to more questions which the aggregate operator cannot answer. In this case, the same process for forwarding the LLR request would be used as if it originally came from their own IT department.

GENI LLR Representative

The GENI LLR Representative's duties are difficult to encapsulate in a simple set of rules. This is because (1) any exceptions not covered in the procedures above will generate a question or request for this person, and (2) this representative will have the most diverse set of requests which could come from any of the other parties discussed. For example, this person may be asked:

- Is *this* a GENI resource and who is responsible for it?
- Who is person responsible for GENI resources at *this* institution and how can I contact them?
- What does *this* software do?
- What does *this* experiment do, and who is responsible for it?
- Why did *this* request come to *me*?
- What is *my* responsibility, according to agreements signed with GENI, in regards to *this* request?

The necessary capabilities defined in the section prior have been noted because these are what the GENI LLR Representative needs to have enough information to answer all of these requests or at least reroute them to people with answers. In fact, the latter is most likely what the representative will do most often in their role as a facilitator. Their job is essentially to gather all the information that they need to create routing

rules or procedures for LLR requests and then to route these requests in such a way that the LLR agent is always at least one step closer to the information they are requesting. The GENI LLR Representative will also be responsible for learning from operational experience with GENI the ways in which these processes and procedures need to be updated, and to maintain this MOU and disseminate changes to it.

Reporting

The GENI LLR Representative will be responsible for generating semi-annual reports about LLR requests. These reports should contain within them statistics to indicate the number of requests, the type of requests, and the successfulness of the resolution process. For *significant* events, defined below, details on the individual requests and their resolution will be provided in these semi-annual reports. These reports will be made public to the GENI community, sanitizing the identity of individuals or organizations involved only upon specific request.

A *significant* LLR event is a request involving more than one slice, a felony criminal investigation or the emergency shutdown of a slice. These events should be reported immediately to the GENI-CSIRT and the GOG outside the regular semi-annual reporting schedule. Of course, in the event of an emergency shutdown, the GENI-CSIRT and GOG would have already been involved as the GENI LLR representative does not have the authority to shut down a slice.

Glossary

- **Aggregate**: is a system containing a collection of resources (i.e. components) under common administration running an aggregate manager service (defined in the GENI Software Framework Architecture).
- **Aggregate Administrator:** is one who has been delegated the responsibility, by the aggregate authority, to set local resource allocation policy for an aggregate and its components.
- **Aggregate Authority (AA):** is responsible for the management of the aggregate, but can delegate selected functions to other actors. The aggregate authority is the one who can enter into agreements for the aggregate.
- **Aggregate Manager:** a service that exports a well-defined remotely accessible control framework interface to an aggregate.
- **Aggregate Operator:** is appointed by the Aggregate Authority to operate the Aggregate Manager and any components of the aggregate. This may be a the AA itself, or someone from another organization operating on its behalf.
- **Component:** encapsulates a collection of resources, including physical resources (e.g., CPU, memory, disk, bandwidth) logical resources (e.g., file descriptors, port numbers), and synthetic resources (e.g., packet forwarding fast paths).
- **GENI-CSIRT:** Computer Security and Incident Response Team for GENI composed of people from several major stakeholder institutions and guided under the authority of the GENI Oversight Group.
- **GENI Project:** is a grouping of experimenters and slices working on a common effort. It may have multiple slices concurrently and over time.
- **GENI Oversight Group (GOG):** is the group responsible for ensuring that meta-operations and the clearinghouse operations groups fulfill their responsibilities. It is also the governance body for the GENI federation, responsible for guiding project direction and resolving disputes between other actors.
- **Identity Portal:** is a trusted (i.e., one that has signed an agreement to collect and verify attributes, use approved identity providers, present users with the AUP, and log credential creation) system that issues GENI credentials for principals.
- **Identity Provider:** is a service providing authentication of potential GENI actors. User registration, vetting, enrollment, and attribute collection will often be exported to an identity provider, such as InCommon, rather than requiring attribution at the identity portal who's main job is minting GENI credentials for those who accept the GENI AUP.
- **Project Leader:** is the actor who is ultimately responsible for the behavior of a GENI project.