G E N I

Global Environment for Network Innovations

Spiral 2 Security Plan

Document ID: GENI-SY-SA-TS-S2-00.1

15 March 2010

Prepared by:
The GENI Project Office
BBN Technologies
10 Moulton Street
Cambridge, MA 02138 USA

Issued under NSF Grant CNS-0741315

TABLE OF CONTENTS

1 Document Scope

This document describes the security plan for GENI Spiral 2.

1.1 Purpose of this Document

The purpose of this document is to document security plans for GENI Spiral 2. It is intended to provide context and direction to Spiral 2 projects, especially the security projects.

The plans presented in this document are motivated by:

1. The tremendous growth of GENI by the end of Spiral 2. By the end of Spiral 2 GENI will have been deployed in over a dozen campus networks and will have over twenty aggregates providing resources for use by experimenters.
2. An increase in the numbers of researchers expected to use GENI for experimentation.

The plans described in this document are Spiral 2 activities in preparation for this growth in GENI by Spiral 3

1.2 Context for this Document

Figure 1 below shows the context for this document within GENI's overall document tree.

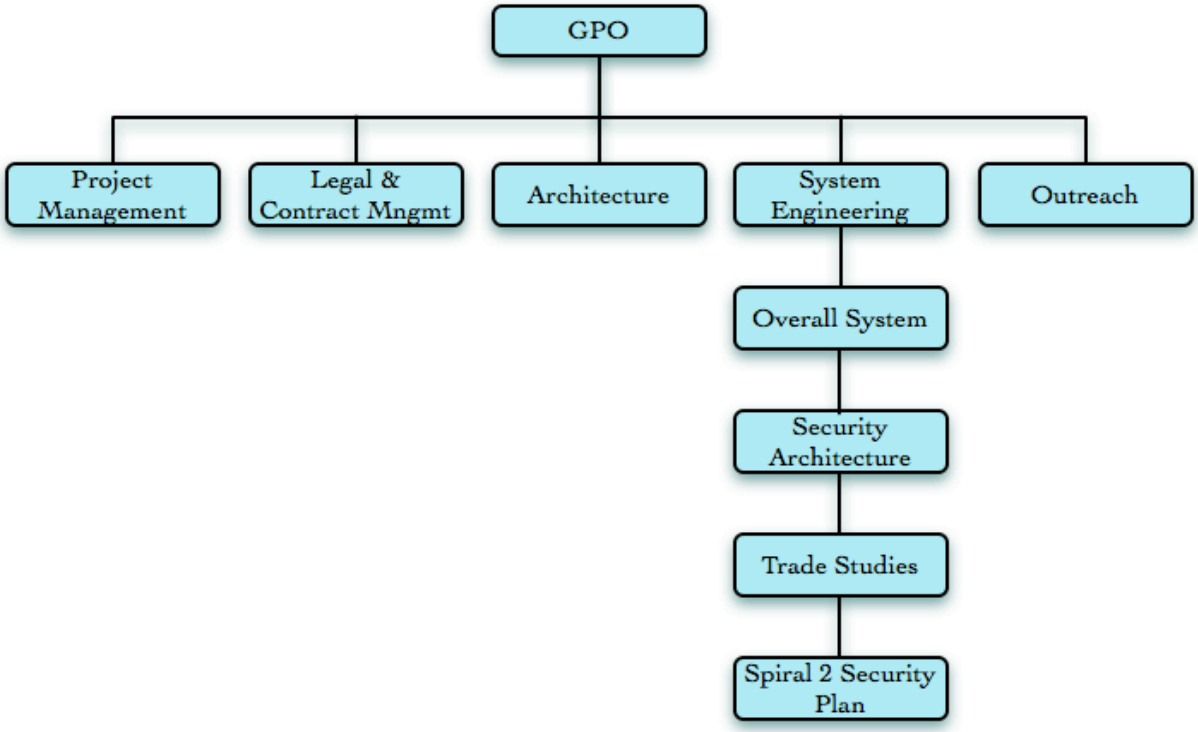

Figure 1. This Document within the GENI Document Tree.

1.3 Related Documents

The following documents of exact date listed are related to this document, and provide background information, requirements, etc., that are important for this document.

1.3.1 National Science Foundation (NSF) Documents

Document ID	Document Title and Issue Date
N / A	

1.3.2 GENI Documents

Document ID	Document Title and Issue Date
GENI-SE-SY-SO-02.0	GENI System Overview

1.3.3 Standards Documents

Document ID	Document Title and Issue Date
N / A	

1.3.4 Other Documents

Document ID	Document Title and Issue Date
Herron	Sprial 2 Emergency Stop Version 4, Jon Paul Herron, http://groups.geni.net/geni/wiki/GENIMetaOps
Peterson	Understanding and Resolving Conflicts on PlanetLab, Larry Peterson
PLConsortium	Joining PlanetLab, May 2007, http://www.planet-lab.org/joining
Slagell	GENI Security Use Cases and Stakeholders , Adam Slagell, January 2010, http://groups.geni.net/geni/attachment/wiki/ComprehensiveSecurityPgm/GENI-Security-Use-Cases-and-Stakeholders.pdf

1.4 Document Revision History

The following table provides the revision history for this document, summarizing the date at which it was revised, who revised it, and a brief summary of the changes. This list is maintained in chronological order so the earliest version comes first in the list.

Revision	Date	Revised By	Summary of Changes
-00.1	11 Mar 10	V. Thomas	Initial draft.

2 GENI Overview

The Global Environment for Network Innovations (GENI) is a novel suite of infrastructure now being designed to support experimental research in network science and engineering.

This new research challenges us to understand networks broadly and at multiple layers of abstraction from the physical substrates through the architecture and protocols to networks of people, organizations, and societies. The intellectual space surrounding this challenge is highly interdisciplinary, ranging from new research in network and distributed system design to the theoretical underpinnings of network science, network policy and economics, societal values, and the dynamic interactions of the physical and social spheres with communications networks. Such research holds great promise for new knowledge about the structure, behavior, and dynamics of our most complex systems – networks of networks – with potentially huge social and economic impact.

As a concurrent activity, community planning for the suite of infrastructure that will support NetSE experiments has been underway since 2005. This suite is termed the Global Environment for Network Innovations (GENI). Although its specific requirements will evolve in response to the evolving NetSE research agenda, the infrastructure's conceptual design is now clear enough to support a first spiral of planning and prototyping. The core concepts for the suite of GENI infrastructure are as follows.

- **Programmability** – researchers may download software into GENI-compatible nodes to control how those nodes behave;
- **Virtualization and Other Forms of Resource Sharing** – whenever feasible, nodes implement virtual machines, which allow multiple researchers to simultaneously share the infrastructure; and each experiment runs within its own, isolated slice created end-to-end across the experiment's GENI resources;
- **Federation** – different parts of the GENI suite are owned and/or operated by different organizations, and the NSF portion of the GENI suite forms only a part of the overall 'ecosystem'; and
- **Slice-based Experimentation** – GENI experiments will be an interconnected set of reserved resources on platforms in diverse locations. Researchers will remotely discover, reserve, configure, program, debug, operate, manage, and teardown distributed systems established across parts of the GENI suite.

As envisioned in these community plans, the GENI suite will support a wide range of experimental protocols, and data dissemination techniques running over facilities such as fiber optics with next-generation optical switches, novel high-speed routers, city-wide experimental urban radio networks, high-end computational clusters, and sensor grids. The GENI suite is envisioned to be shared among a large number of individual, simultaneous experiments with extensive instrumentation that makes it easy to collect, analyze, and share real measurements.

3 GENI Security Context

GENI faces security challenges that are different from those faced by typical enterprise networks. GENI features that differentiate it from typical enterprise networks include:

- GENI is not owned and operated by one legal entity
- GENI users belong to different organizations
- GENI resources are much more diverse than the typical hosts and network devices on enterprise networks
- GENI users can program almost any resource on the network, including network devices
- GENI is designed to be much more configurable than any enterprise network, which means it is more prone to errors in configuration.
- GENI connects to the Internet in a large number of places that are controlled by different organizations.

The scale of GENI, in terms of its number of resources and their geographic spread, makes it an attractive launch pad for large-scale attacks. The national and international attention garnered by the GENI project makes it an attractive target for attacks, for bragging rights if not anything else. The use of GENI for virtually any kind of networking experiment, including long-lived experiments, makes it an attractive platform for hiding and distributing illicit content.

3.1 GENI Security Stakeholders

GENI has a number of different stakeholders, each with a different objective for GENI security. These stakeholders and their security objectives are summarized in **Error! Reference source not found.**. Adam Slagell of the NCSA has a similar analysis of GENI stakeholders [Slagell].

The National Science Foundation (NSF), as the government agency funding the GENI project, and BBN Technologies, as the organization providing project management and systems engineering for

Stakeholder	Security Objectives
NSF/BBN	GENI not used for illegal activity or as launchpad for attacks. GENI availability not compromised by attacks.
Control framework developers	Control framework functions not hijacked to gain unauthorized access to resources.
Aggregate providers	Information needed to enforce resources usage policies is available and trustworthy (who, when, how much). Resources not used for illegal activities or as launchpad for attacks.
GENI Ops	Quickly learn about incidents. Ability to determine scope and severity of threat. Ability to contain/eliminate threat. Procedures for responding to requests from law-enforcement.
Experimenters	Experiment privacy (nature of experiment, data). Resource availability.
Opt-in users	Privacy agreements are honored.
Campus IT	Campus security and privacy policies are not violated.
Federation Partners	Security compromises/attacks don't cross federation boundaries. Resources usage policies are adhered to (who, when, how much). Resources not used for illegal activities or as launchpad for attacks.

Table 1. GENI security must meet the needs of its different stakeholders.

GENI, are both keenly interested in keeping GENI from being used for illegal activities or as a launch pad for attacks. Not only will such activities result in very bad press, they will setback progress in the Network Science research by delaying the construction of any large networking infrastructure. Additionally, the NSF and BBN Technologies are interested in GENI serving its purpose i.e. being available for experimentation by researchers. They want GENI to be secure and be highly available for research.

The GENI control framework developers are primarily interested in ensuring their GENI control plane does not have vulnerabilities that can be used to attack GENI or to get unauthorized access to its resources.

Almost all GENI resources are provided by its various aggregate providers. These providers have a vested interest in ensuring resources made available for GENI are used only by GENI researchers for their intend purposes. Aggregates must have the information necessary to know who is using their resources and to enforce any resource usage policies.

GENI Operations consists of operations staff from the aggregates providing resources to GENI and staff from the GENI Meta-Operations Center. GENI Operations therefore spans multiple organizations with the GENI Meta-Operations Center coordinating the actions of this distributed operations team. GENI Operations needs to quickly learn about security-related incidents, determine the scope and severity of the threat, and contain the threat. GENI Operations must also have the procedures in place to respond to legal-threats or to requests from law-enforcement agencies.

GENI experimenters expect the nature of their experiments and data used and generated by their experiments be kept private. This is especially important to experiments that use private data from individuals; experimenters and Institutional Review Boards (IRBs) must have a reasonable expectation that unauthorized personnel cannot access this private data.

Opt-in users are not necessarily GENI researchers. They are people who have signed up to use experimental services provided by GENI or to participate in an experiment on GENI. Opt-in uses typically sign agreements with the GENI researcher conducting the experiment or hosting the experimental service that cover, among other things, how private data about the user will be used. Opt-in users and GENI experimenters must have a reasonable expectation that vulnerabilities in GENI will not cause these agreements to be violated.

As GENI is deployed in campuses around the country, campus policies related to the use of information on the network must not be honored. This is of particular concern is ensuring these policies are not violated by Internet feeds to GENI experiments.

Finally, GENI will federate with similar infrastructures such as testbeds being developed by other nations or commercial testbeds. GENI and its federation partners will have the expectation that security compromises and attacks do not cross federation boundaries. Additionally, federation partners will expect that GENI has taken reasonable measures to verify assertions made by GENI about its users wishing to use federation resources.

4 GENI Spiral 2 Security Objectives

As stated in Section 1.1, the primary objective of the GENI Spiral 2 security plan is to prepare for the tremendous growth in GENI by the end of the spiral. Growth in Spiral 2 comes from GENI deployments in over a dozen campuses (with about a dozen more planned for Spiral 3) and from over twenty aggregates associating themselves with GENI. The number of researchers using GENI is also

expected to grow by Spiral 3. Some researchers are using GENI for standing up experimental services for opt-in users; the numbers of these opt-in users too will increase as these services mature and gain in popularity.

As GENI grows in size and popularity, so does the importance of a dedicated operations team tasked with ensuring GENI remains a safe and reliable infrastructure for research and experimentation. The fact that the GENI operations team consists of members from multiple organizations with different priorities and with different levels of experience and expertise with operations presents some unique challenges.

Good policies and procedures with well-defined roles, responsibilities and expectations are essential for a diverse and distributed operations team to be effective. The GENI Spiral 2 security plan therefore focuses on putting together procedures that will allow the GENI operations team to work together to prevent security incidents and to deal with such incidents should they occur. The specific procedures to be developed in the spiral are described in Section 6.

5 The GENI Operations Team

The GENI system architecture includes *aggregates*, which are collections of resources available to researchers using GENI for running experiments. Aggregates are owned by *aggregate providers*, which are groups such as research labs, university departments, universities or commercial entities. Aggregates are associated with the GENI *clearinghouse*. The clearinghouse lists resources made available to GENI researchers by its associated aggregates and also maintains inventories of resources held by researchers using GENI. [GENI-SE-SY-SO-02.0]

The GENI operations team includes members of the network or systems administration staff of the aggregate providers associated with the GENI clearinghouse. They may be members of the research group that maintains the aggregate or members of the IT staff of the aggregate provider's organization. GENI operations team members may therefore run the gamut from researchers with little or no operations experience to full-time professional IT personnel.

The GENI operations team also includes members of the GENI Meta-Operations Center. This is a professionally staffed organization with overall responsibility for GENI operations. Staff at the GENI Meta-Operations center monitor GENI and take appropriate actions to ensure GENI is meeting its operational objectives. Some of these operational objectives include security objectives such as ensuring GENI resources aren't being used by unauthorized users or GENI isn't being used as a launch-pad for attacks.

The GENI Meta-Operations center is responsible for coordinating the actions of the members of the GENI operations team, which as described earlier, belong to different aggregate provider organizations.

It should be noted that the GENI clearinghouse might federate with other clearinghouses. These clearinghouses would have their own operations structure. Formal agreements and processes will need to be place to for coordinating actions across these operations teams and for sharing operations-related information. These agreements are processes are outside the scope of this document and will not be addressed in Spiral 2.

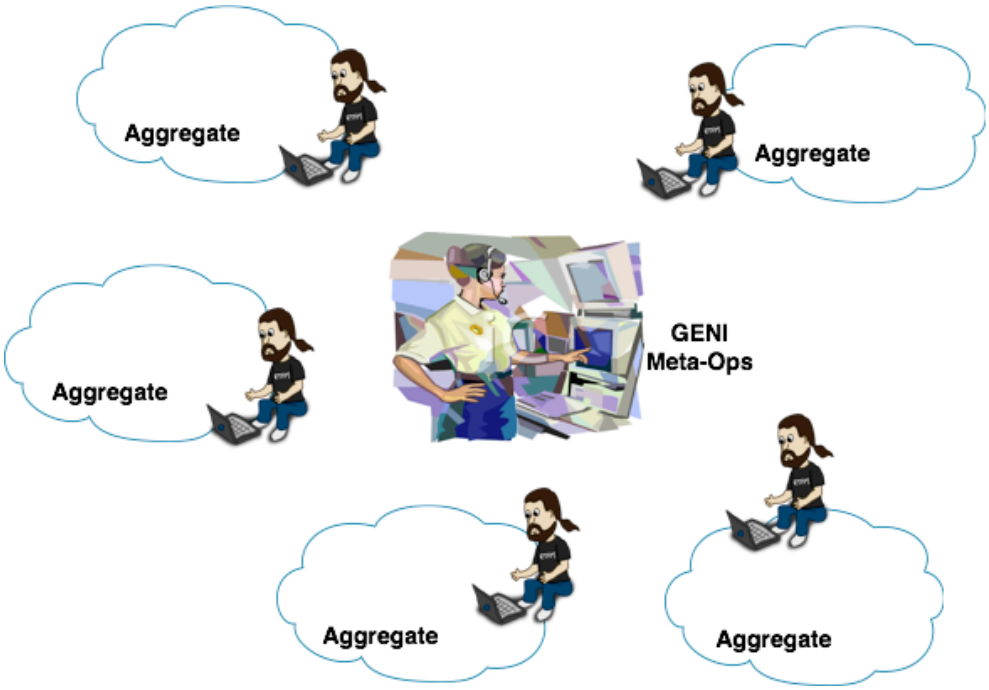

Figure 1. The GENI Meta-Operations Center coordinates the actions of the GENI Operations team that includes members from the various aggregate providers.

6 GENI Spiral 2: Security Operations Related Procedures

As mentioned in the previous section, the GENI security plan for Spiral 2 is focused on developing procedures for the distributed GENI operations team to prevent security incidents and address them should they occur. The following documents will be developed in this spiral:

1. An aggregate provider agreement,
2. Security best practices for aggregate providers,
3. Emergency stop procedures,
4. Procedures for responding to threats of legal action or law enforcement requests.

These documents are described in the remainder of this section.

6.1 The Aggregate Provider Agreement

The *Aggregate Provider Agreement* is an agreement between the clearinghouse and an aggregate that associates itself with the clearinghouse. Aggregate resources cannot be discovered or used by GENI researchers using the clearinghouse until this agreement is in place.

This agreement will cover the clearinghouse operator's expectations of the aggregate provider. This may include expectations about who can or cannot be denied access to aggregate resources and minimum organizational and security structures that must be in place to assist with GENI operations.

The agreement may also cover aggregate provider's expectations of the clearinghouse. This may include expectations about the users authorized to request resources from the clearinghouse,

mechanisms used to verify the identity of these users, and information about these users that will be made available to the aggregates.

The process of developing this agreement needs to identify the parties to the agreement. Specifically, for the GENI clearinghouse, what might me the legal entity that operates this clearinghouse and how is it funded. For the aggregate provider side of the agreement, it will presumably be signed by a representative of a legal entity such as the university/organization providing the resources.

This task of drafting this agreement will draw on the existing GENI Recommended Use Policy, the PlanetLab consortium documents [PLConsortium], and documents related to membership of the various grid-computing consortia.

6.2 Security Best Practices for Aggregate Providers

The *Security Best Practices* document will provide guidance to aggregate providers on securely managing portions of their network that affect GENI security. This may include the appropriate of firewalls, management of user logins, and suitable separation of GENI resources from operational resources within the aggregate provider's network.

It is expected there will be a core best practices document that applies to all aggregates. There will be addendums to this core document with specific best practices for different types of aggregates such as wired aggregates and wireless aggregates.

This task will draw on the security practices of existing testbeds such as PlanetLab, Emulab and ORBIT and on security best practices in enterprise networks.

6.3 Emergency Stop Procedures

This document will lay out the procedures used to coordinate actions of the GENI operations team to stop suspicious traffic to or from a GENI resource. An objective is to stop the traffic with minimum disruption to on-going experiments that are not involved with the suspicious traffic.

The procedure will have to account for the very real possibility that one or more aggregates may not respond in a timely manner to requests to take certain actions related to stopping suspicious traffic. This may be due to a reasons such as aggregates not be staffed around the clock with operations personnel to the operations staff at an aggregate concerned about the impact of their actions on other organizational objectives.

This task will draw on the Sprial 2 Emergency Stop requirements document developed by the GENI Meta-Operations project [Herron].

6.4 Procedures for Responding to Threats of Legal Action or Law Enforcement Requests

This document will describe procedures used to coordinate the actions of the GENI operations team to respond to threats of legal action or requests for information from law enforcement agencies. Because IP traffic from GENI resources typically contain source addresses from the address space of the organization owning the resource, the threat of legal action or the law enforcement request will likely go to the aggregate provider's IT department rather than the organization of the researcher running the experiment that is using the resource. The procedure will cover action taken to identify the slice owning the resource that is the target of the legal action, the researcher owning the slice, and developing an appropriate plan to investigate the incident. Slice related information may have to be collected and archived to support future investigations or legal actions. The procedure must account for

different aggregate providers having different internal policies on who conducts these investigations and how they are conducted.

This task will draw on experiences of existing testbeds such as PlanetLab on handling such requests [Peterson].

7 Acronyms

The following table defines acronyms used within the GENI Project.

GENI	Global Environment for Network Innovations