GridPP
UK Computing for Particle Physics

LHC OPN Security Policy

Robin Tasker (r.tasker@dl.ac.uk)
CCLRC, Daresbury Laboratory

14 November 2005

National e-Science Centre

CCLRC Daresbury Laboratory

Summary of Security Policy

Assumptions Intended Audience	*Setting the Scene*
Scope	*Setting the Context*
Roles and Responsibilities Legislation and Compliance	*Spelling out the Governance*
IP Routing IP Protocols Access Control	*The technical stuff of the policy*
Incident Handling and Reporting	*Procedural matters*
Open Questions	*Still up for discussion!*

Key Components of Policy

Assumptions	*1. Each site will decide what is and is not acceptable with respect to Information Security.* *2. Existing LCG/EGEE Security Policy and procedures will be followed.* *3. Site access to the OPN available only after agreement to follow this OPN IS Policy.*
Scope	*1. This Policy specifies the rules which determine whether or not a site is permitted to transmit data across the OPN.* *2. This Policy mandates a site to police and enforce the rules on the reception.* *3. Membership of the OPN is restricted to the Tier 0 and Tier 1 sites.* *4. Any other use of the OPN is deprecated. Any traffic resulting from such use may be discarded without warning or notification.*

Key Components of Policy

Roles and Responsibilities	*1. Each site will nominate a suitable person and deputy to represent the site's interests with respect to the provision of security on the OPN.* *2. The IS Officer at each OPN site will be satisfied with the mitigation of any IS risk associated with that site's connection to the OPN.* *3. The OPN security representatives will be responsible for on-site liaisons with the local site to obtain a formal record of acceptance and implementation of this policy.*
Legislation and Compliance	*1. Each site will act in accordance with any national or international legislation applicable in that country to the operation of a data network.* *2. The OPN security representatives will work with the local site IS Security officer to demonstrate compliance with this Policy.*

Key Components of Policy

IP Routing	*1. Specifies general BGP rules for the Tier sites* *2. Specific Tier 0 BGP configuration rules* *3. Specific Tier 1 BGP configuration rules* *4. Rules for non-OPN traffic – no transit here!*
IP Protocols	*1. IP, TCP and UDP allowed* *2. Application level protocols to support LHC data exchange between the Tier sites allowed* *3. Protocols to support the operation of the OPN, e.g. ICMP, SNMP, PMTUD traffic, allowed*
Access Control	*1. Requirement to use either an Access Control List (ACL) or similar technical process, e.g. a firewall, to deliver this Security Policy* *2. Each site will deploy access control on received traffic based upon that site's IS Security policy.* *3. Outbound traffic subject to access control* *4. Inbound traffic policed to meet the site IS Policy*

Key Components of Policy

Incident Handling and Reporting	*1. For security incidents, LCG sites have an agreed policy and procedure.* *2. A new incident response handling procedure is currently being processed through the LCG and EGEE.* *3. This Policy follows these procedures!*
Open Questions	*1. Domain name services for the LHC OPN* *2. Disaster/emergency planning for LCG/EGEE is under discussion and needs to be addressed for the LHC OPN.* *3. Business continuity planning.*

What Happens Next?

Agree this Security Policy	*1. Receive and incorporate comments on Draft 4; circulate the revision and publish as Final text*
Fill in the Gaps	*1. Table 1: Specify membership of the OPN together with the associated CIDR prefixes* *2. Table 2: Specify the OPN Security representatives for each site.*
Access Control	*1. Specification of BGP environment for the OPN* *2. Generate "generic" access control "rules" as advice for site-specific implementation.*
Engagement	*1. Liaison with, and agreement from, site IS Security officers.* *2. Compliance…just do it!*
Open Questions	*1. DNS needs to be incorporated into the OPN now* *2. Disaster recovery / BCP needs to be progressed in parallel and be ready for the off..*