NETWORK SECURITY

Focus Area Session Chair	Hank Kluepfel
Focus Area Champion:	Gary Luckenbaugh
Focus Area Editor:	Hank Kluepfel
Participants	

I. DEFINITION

Network Security is the surveillance, protection, containment, and deterrence of abuse against assets. This should be within the context of a risk management framework.

Network Security is the property of the network that ensures.

1. Protection
   - Confidentiality
   - Integrity
2. Accountability
3. Availability against internal or external threats

Network Security is both a term and an attribute related to the protection, detection and containment of physical and logical threats to network information, network resources and communication including data. systems, applications, centers and human/machine interfaces with respect to availability, confidential, integrity, access control, authentication, audit and recovery. It is also an attribute of quality and reliability in relation to the value of the asset to be protected or the criticality of asset to the business.

Network Security in essence is an extension of the internal set of controls reflective of both industry standards and best practices. It involves inferred trust, roles, relationships, responsibilities, and accountabilities for intra-network as well as inter-networks.

Network Security is an essential component of the application, transport, network management, and configuration management. It, like quality, is a journey not a destination.

Network Security is not only information security and physical security but also a combination of both disciplines addressed to the nodes, links, paths and databases.

Network Security is not easy but is not rocket science.

Network Security is not a last minute activity, a road block to legitimate use, absolute, free, a maintenance feature, and to impair other features of the system.

II. METRICS

Network Security can measured by . . .

- Number of incidents by type (e.g. Motive, impact)
- Penetration testing (e.g. Dial of access, building access, password aging)
- Audit
- Cost of security failure (direct and indirect)

Network Security can best be measured by a combination of the frequency and severity (both direct and indirect consequences) of failures to prevent, detect or contain threats to network resources and information. Network Security can best be measured by compliance testing and benchmarking against industry standards.

III. PARTICIPANTS

The working group participants consisted of the following industry professionals.

NAME	AFFILATION
Dietl, Thomas	Deutsche Telekom AG
Duell, Kenneth	AT&T
Harrison, John	BT System Engineering
Kluepfel, Henry	Science Applications International Corp
Luckenbaugh, Gary	Lockheed Martin Mission Systems
Macwan, Anil	Lucent Technologies
Makris, Spilios	Bell Communications Research
Murata, Masayuki	Osaka University
Perris, Eve	Bell Communications Research
Walling, Kenneth	Pacific Bell
Yu, Weider	Lucent Technologies