White Paper

Approaches for Applying Robustness Levels to the GIG IA RCD Attributes

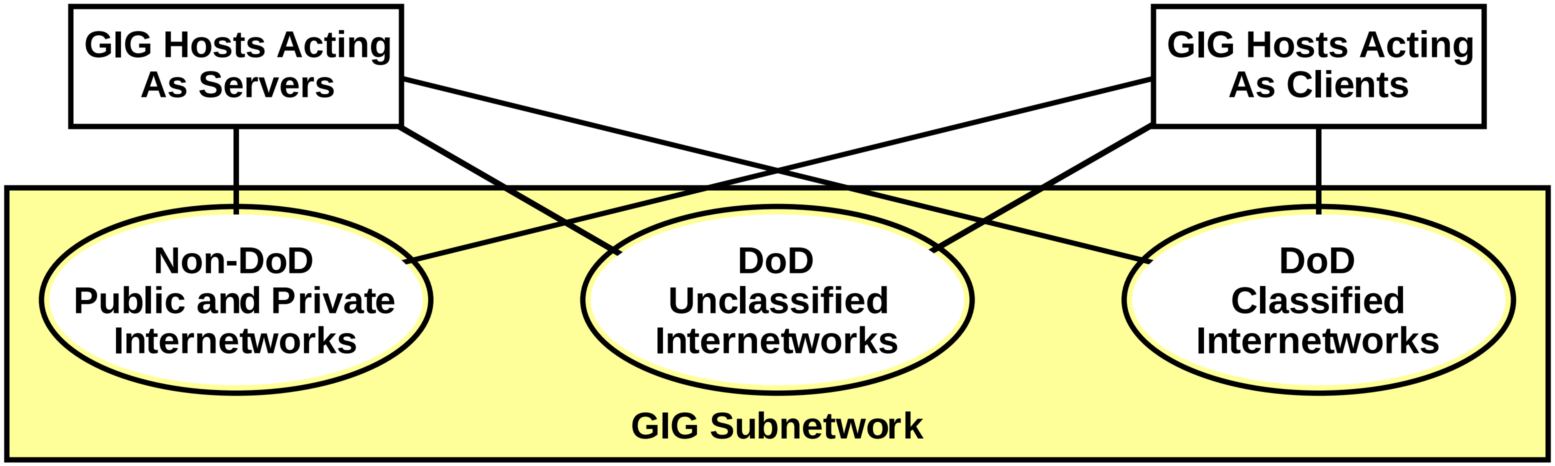
1 December 2004

R.W. Shirey
BBN Technologies
Arlington, Virginia
<rshirey@bbn.com>

Evolution of DoD Policy for Robustness

- **Criteria for security features and assurances**
  - – TCSEC (Orange Book), Yellow Book, and DoDD 5200.28
  - – DCID 6/3 – Confidentiality, Integrity, Availability
    - Levels of Concern, Protection Levels, Controls
  - – DoDI 8500.2 – Confidentiality, Integrity, Availability
    - Mission Assurance Categories, Confidentiality Levels, Controls
    - Defense in Depth, Robustness Levels, Common Criteria
  - – NIST Special Publication 800-53
- **Newest guidelines don’t incorporate a risk index**
  - – Highest valued resource versus lowest authorized user
  - – Necessary controls versus sufficient controls
- **GIG robustness cannot be uniform or unique**
  - – Must support alternatives; policy must build on ordinary rules
  - – Ensure high robustness for special IA functions/components
  - – Ensure floor of robustness for widely performed IA functions

Figure 1. GIG Computer Network


GIG Hosts Acting As Servers
GIG Hosts Acting As Clients
Non-DoD Public and Private Internetworks
DoD Unclassified Internetworks
DoD Classified Internetworks
GIG Subnetwork

- **Component subsystems of the host layer**
  - – IA-specific: A few that provide IA services for all GIG users.
  - – Non-IA: Vast majority, which support non-IA applications.
- **Component subsystems of the subnetwork layer**
  - – Primary networks: A few long-haul, common-use, at different classification levels or under authority of different agencies.
  - – Secondary networks: Thousands of MANs and LANs to serve specific communities separated by geography or organization.

Fig 2. GIG Subnetwork Layer

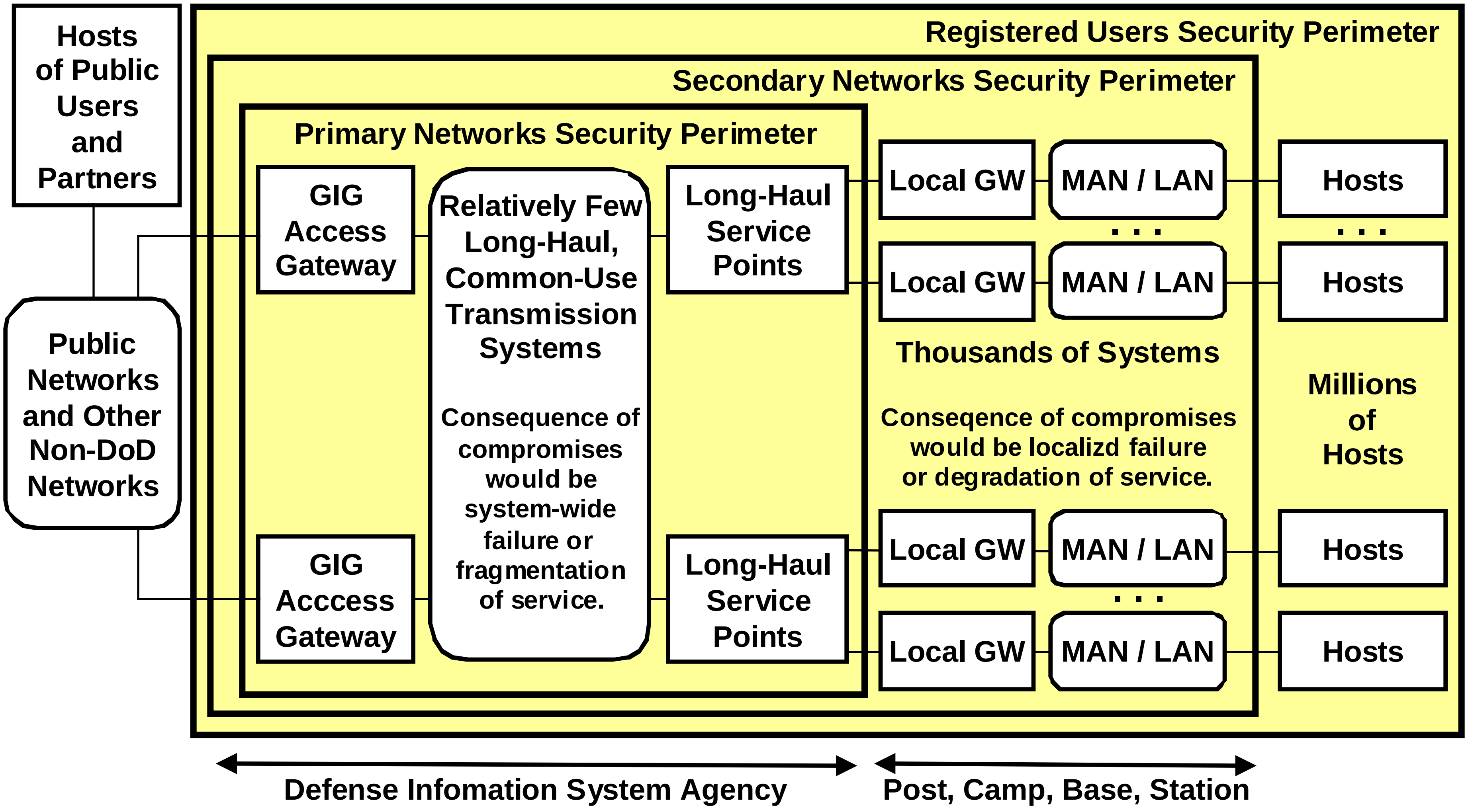
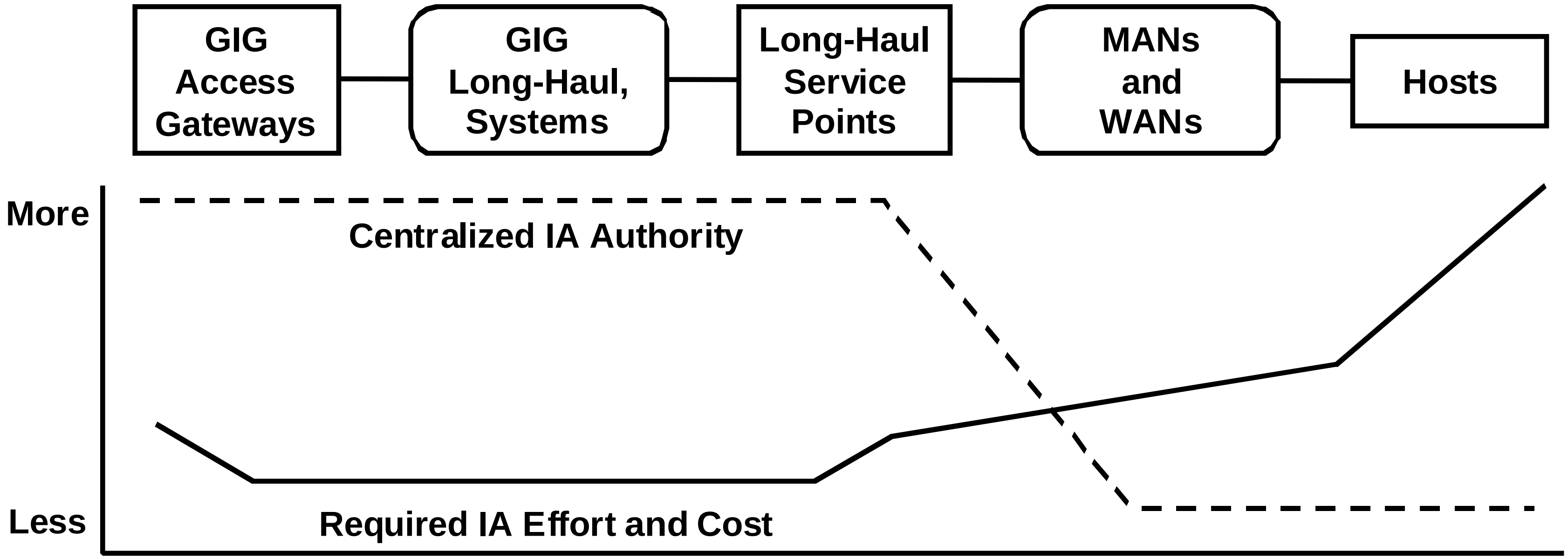
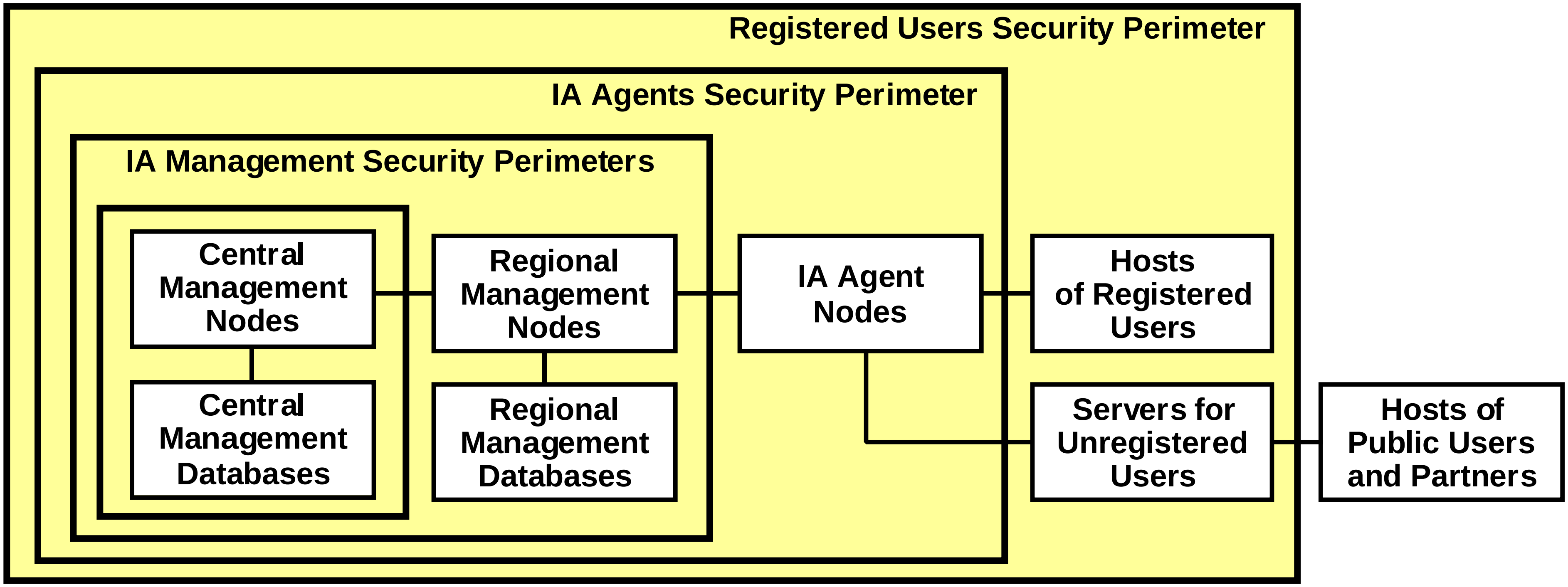

Hosts of Public Users and Partners
Public Networks and Other Non-DoD Networks
Registered Users Security Perimeter
Secondary Networks Security Perimeter
Primary Networks Security Perimeter
GIG Access Gateway
GIG Acccess Gateway
Relatively Few Long-Haul, Common-Use Transmission Systems
Consequence of compromises would be system-wide failure or fragmentation of service.
Long-Haul Service Points
Long-Haul Service Points
Local GW
MAN / LAN
Hosts
. . .
Local GW
MAN / LAN
Hosts
Thousands of Systems
Conseqence of compromises would be localizd failure or degradation of service.
Millions of Hosts
Local GW
MAN / LAN
Hosts
. . .
Local GW
MAN / LAN
Hosts
Defense Infomation System Agency
Post, Camp, Base, Station

Fig 3. Mismatch of Effort vs. Authority



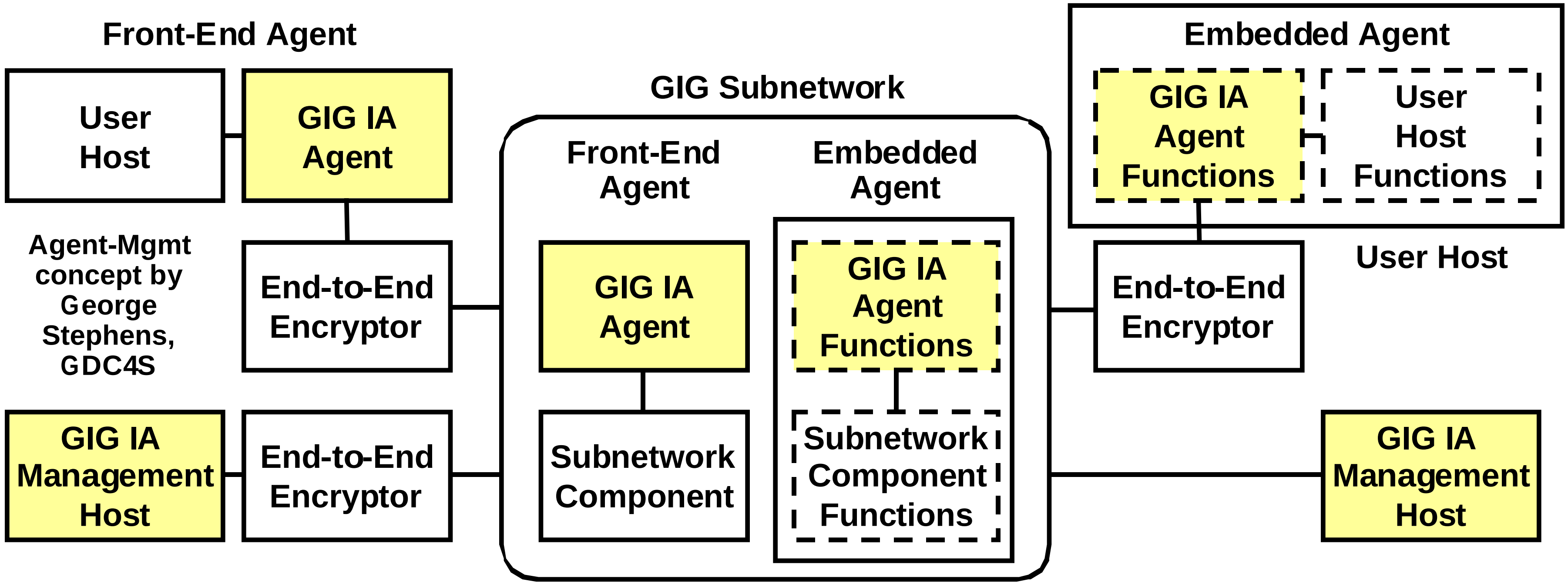
- Most IA resources are deployed in places where DoD core management lacks effective means to coordinate the resources for maximum effect.
- Outer perimeter in Figure 2 is so long and diffuse that it has proven nearly impossible to organize a strong defense in a cost-effective manner.

Fig 4. GIG Host Layer


Registered Users Security Perimeter
IA Agents Security Perimeter
IA Management Security Perimeters
Central Management Nodes
Central Management Databases
Regional Management Nodes
Regional Management Databases
IA Agent Nodes
Hosts of Registered Users
Servers for Unregistered Users
Hosts of Public Users and Partners

- IA agent node: Closely associated with one (or a few) hosts to provide IA service (e.g., RAdAC PEP).
- IA management nodes: Regionalized or centralized to manage or support agents (e.g., RAdAC PDP)
- Model applies recurrently if hierarchical managers

Fig 5. GIG IA-Specific Subsystem Nodes



- Embedded agent: When host platform has enough robustness to support the IA functionality.
- Front-end agent: If higher robustness needed for IA.
- Example: HAIPE is an agent node in (1) subsytem for end-to-end transmission security and (2) subsystem for key management and distribution (a.k.a. KMI).

Table 1. Availability and Integrity

Security Property	IA Subsystem Agent Node		IA Subsystem Management Node
	Viewed As a Part of the User Host	Viewed As a Part of the Subsystem	
	Combine the controls from these two columns (and use the stronger control where they differ).		
Availability	Assign same DoDI 8500.2 MAC as is assigned to the user host: MAC I, II, or III. Apply the DoDI 8500.2 controls of that MAC .	Assign the DCID 6/3 LOC that is comparable to the MAC of the user host , where MAC I = High, II = Medium, III = Basic. Apply the DCID 6/3 controls of that LOC .	Assign a DCID 6/3 Availability LOC: High, Medium, or Basic. (High LOC is expected in most subsystems.) Apply the DCID 6/3 controls of that LOC .
Integrity		Assign same DCID 6/3 LOC that is assigned to management nodes: High, Medium, or Basic. (Might be lower than for managment nodes if management is MLS.) Apply the DCID 6/3 controls of that LOC	Assign a DCID 6/3 Integrity LOC: High, Medium, or Basic. (High LOC is expected in all subsystems.) Apply the DCID 6/3 controls of that LOC .

Table 2. Confidentiality Levels for Nodes

Security Property	IA Subsystem Agent Node		IA Subsystem Management Node
	Viewed As a Part of the User Host	Viewed As a Part of the Subsystem	
	Combine the controls from these two columns (and use the stronger control where they differ).		
Confidentiality	Regarding user data traffic handled by the Agent: Assign same DoDI 8500.2 Confidentiality Level as is assigned to the user host: Class., Sensitive, Unclass. (Might be lower than user host if host is MLS. Might be higher if agent must filter data sent to host.) Apply the DoDI 8500.2 controls of that Level .	Regarding subsystem data handled by the Agent: Assign a DoD 8500.2 Confidentiality Level: Class., Sensitive, Unclass. (Might be lower than for managment nodes if management is MLS.) Apply the same DCID 6/3 PLs as for management nodes .	Regarding subsystem data handled by Management: Assign a DoD 8500.2 Confidentiality Level: Class., Sensitive, Unclass. Apply the DCID 6/3 PLs: If Unclass, apply PL 1. If Sensitive, see Table 3 (i.e., PL 1, 2, or 3). If Classified, see Table 3 (i.e., PL 1, 2, 3, 4, or 5.).

Table 3. Robustness Levels for Nodes

If the lowest clearance among the node’s users is ...	and the formal access approval of the node’s users is ...	and the need to know of the node’s users is ...	then apply this Protection Level.
At least equal to the highest data.	All users have all access approvals.	All users have need to know for all data.	PL 1 (Lowest)
At least equal to the highest data.	All users have all access approvals.	Some user does not need to know all data.	PL 2
At least equal to the highest data.	Some user is not approved for all data.	[Does not matter.]	PL 3
Some user is not cleared for all data. Note: DCID 6/3 has “Secret” here.	[Does not matter.]	[Does not matter.]	PL 4
Some user has no clearance at all.	[Does not matter.]	[Does not matter.]	PL 5 (Highest)