

# Robustness Strategy Application



Teri Arber  
Deb Cooley  
Steve Hirsch  
Jim Osterritter

# The Case Study

---

---

- Describe the Roles
- Describe the System
- Define the Security Policy
  - Information Value
  - Threat Environment
- Limit the Architectural Options
- Apply the Robustness Strategy Process

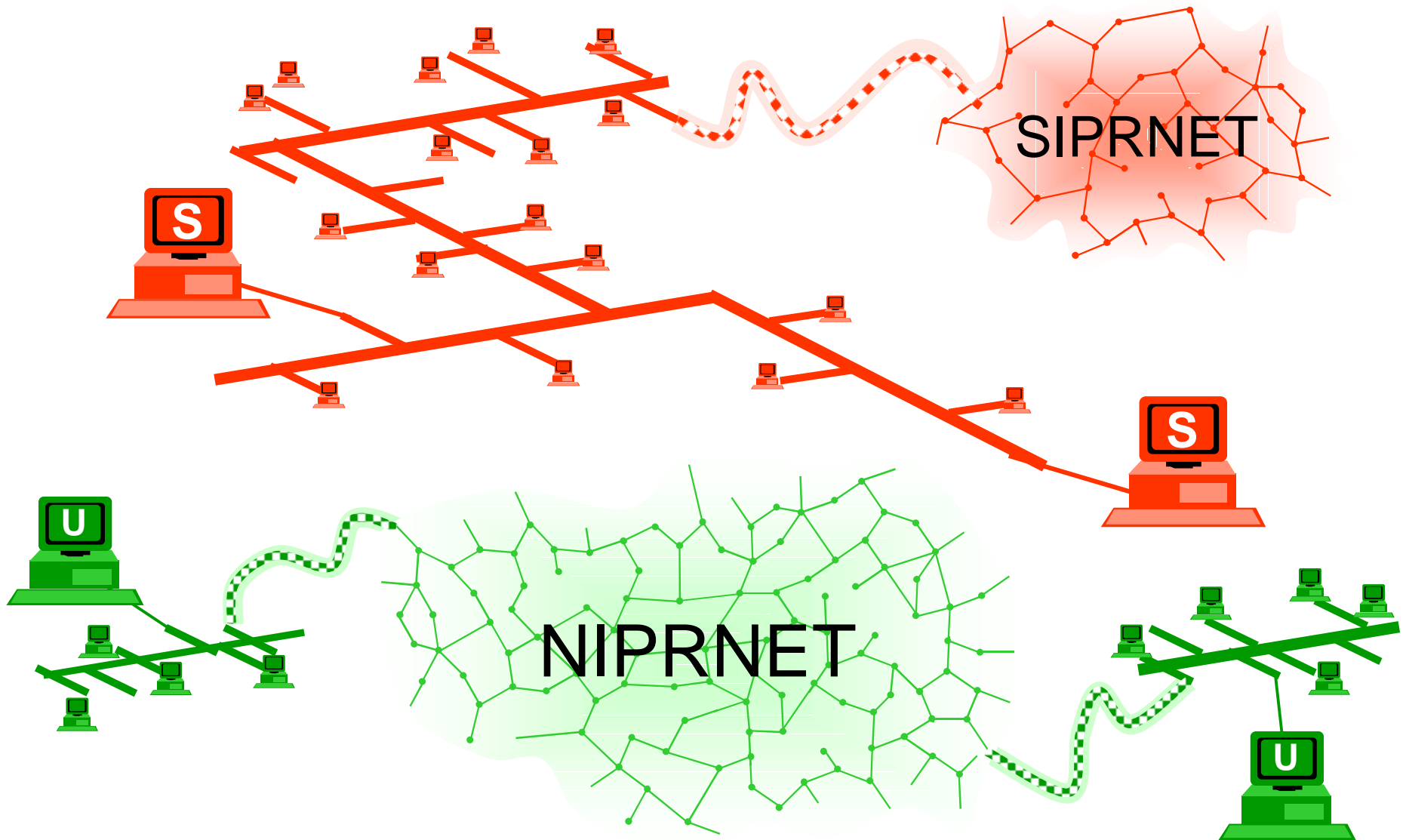
# Describe the Roles

---

---

- Deb Cooley - Facilitator
- Jim Osterritter - ISSE
- Steve Hirsch - Accreditor
- Teri Arber - Customer
- Audience - Jury

# Describe the System



8 December 99

IATF: Robustness Strategy

# Describe the System

---

---

- There is a global, reliable, secret system high network processing a wide variety of data types.
- This network has an unreliable connection to SIPRNET.

# Describe the System

---

---

- There are many small unconnected reliable unclassified networks with unclassified users processing highly formatted data.
- These networks have unreliable connections to NIPRNET.

# Describe the System

---

---

- The goal is to provide a *global*, reliable, unclassified network with unclassified users processing highly formatted data.

# Current Security Policy

---

---

- Secret information must be protected against unauthorized disclosure and modification.
- Secret network must be available when needed.
- Unclassified information does not require protection.

# Desired Security Policy

---

---

- Secret information must be protected against unauthorized disclosure and modification.
- Secret and unclassified information must be available when needed.

# Limit the Architectural Options

---

---

- Customer cannot afford to duplicate the Secret network to offer a global Unclassified network.
- Customer cannot afford to clear all Unclassified users to Secret.
- Customer cannot change the Secret network (e.g., can't add security functions or change operational policy).

# Limit the Architectural Options

---

---

- Tunnel Unclassified information through Secret network
- Connect the two networks with Guards

# Robustness Strategy Process

---

---

- Determine the Value of Information
- Determine the Threat Environment
- Determine the Degree of Robustness
- Select Security Services
- Select Security Mechanisms
- Assess Residual Risk

# Determine Information Value

---

---

- V1: Negligible adverse effects
- V2: Minimal damage
- V3: Some damage
- V4: Serious damage
- V5: Exceptionally grave damage

# Determine Information Value

---

---

- V1: Negligible adverse effects
- V2: Minimal damage
- V3: Some damage
- **V4: Serious damage**
- V5: Exceptionally grave damage

# Determine Threat Environment

---

---

- T1: Inadvertent or accidental
- T2: Casual adversary, min. resources, little risk
- T3: Adversary, minimal resources, significant risk
- T4: Sophisticated, moderate resources, little risk
- T5: Sophisticated, moderate resources, sig. risk
- T6: Very sophist., abundant resources, little risk
- T7: Very sophisticated, abundant resources, significant risk

# Determine Threat Environment

---

---

- T1: Inadvertent or accidental
- T2: Casual adversary, min. resources, little risk
- T3: Adversary, minimal resources, significant risk
- T4: Sophisticated, moderate resources, little risk
- T5: Sophisticated, moderate resources, sig. risk
- **T6: Very sophist., abund. resources, little risk**
- T7: Very sophisticated, abundant resources, significant risk

# Determine Degree of Robustness

| Info.<br>Value | Threat Levels |              |              |              |              |              |              |
|----------------|---------------|--------------|--------------|--------------|--------------|--------------|--------------|
|                | T1            | T2           | T3           | T4           | T5           | T6           | T7           |
| V1             | SML1<br>EAL1  | SML1<br>EAL1 | SML1<br>EAL1 | SML1<br>EAL2 | SML1<br>EAL2 | SML1<br>EAL2 | SML1<br>EAL2 |
| V2             | SML1<br>EAL1  | SML1<br>EAL1 | SML1<br>EAL1 | SML2<br>EAL2 | SML2<br>EAL2 | SML2<br>EAL3 | SML2<br>EAL3 |
| V3             | SML1<br>EAL1  | SML1<br>EAL2 | SML1<br>EAL2 | SML2<br>EAL3 | SML2<br>EAL3 | SML2<br>EAL4 | SML2<br>EAL4 |
| V4             | SML2<br>EAL1  | SML2<br>EAL2 | SML2<br>EAL3 | SML3<br>EAL4 | SML3<br>EAL5 | SML3<br>EAL5 | SML3<br>EAL6 |
| V5             | SML2<br>EAL2  | SML2<br>EAL3 | SML3<br>EAL4 | SML3<br>EAL5 | SML3<br>EAL6 | SML3<br>EAL6 | SML3<br>EAL7 |

# Determine Degree of Robustness

| Info.<br>Value | Threat Levels |              |              |              |              |              |              |
|----------------|---------------|--------------|--------------|--------------|--------------|--------------|--------------|
|                | T1            | T2           | T3           | T4           | T5           | T6           | T7           |
| V1             | SML1<br>EAL1  | SML1<br>EAL1 | SML1<br>EAL1 | SML1<br>EAL2 | SML1<br>EAL2 | SML1<br>EAL2 | SML1<br>EAL2 |
| V2             | SML1<br>EAL1  | SML1<br>EAL1 | SML1<br>EAL1 | SML2<br>EAL2 | SML2<br>EAL2 | SML2<br>EAL3 | SML2<br>EAL3 |
| V3             | SML1<br>EAL1  | SML1<br>EAL2 | SML1<br>EAL2 | SML2<br>EAL3 | SML2<br>EAL3 | SML2<br>EAL4 | SML2<br>EAL4 |
| V4             | SML2<br>EAL1  | SML2<br>EAL2 | SML2<br>EAL3 | SML3<br>EAL4 | SML3<br>EAL5 | SML3<br>EAL5 | SML3<br>EAL6 |
| V5             | SML2<br>EAL2  | SML2<br>EAL3 | SML3<br>EAL4 | SML3<br>EAL5 | SML3<br>EAL6 | SML3<br>EAL6 | SML3<br>EAL7 |

# Select Security Services

---

---

- Confidentiality
- Integrity
- Availability
- Identification and Authentication
- Access Control
- Accountability
- Non-Repudiation
- Security Management

# Select Security Services

---

---

- **Confidentiality**
- **Integrity**
- **Availability**
- Identification and Authentication
- Access Control
- Accountability
- Non-Repudiation
- **Security Management**

# Confidentiality Mechanisms

|             | Cryptographic Algorithm                                                      |                                                                                           | Physical Security        | Technical Security         |                                                                      | Anonymity                                       |                   |
|-------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|--------------------------|----------------------------|----------------------------------------------------------------------|-------------------------------------------------|-------------------|
|             | Effective Key Length                                                         | Key Management                                                                            |                          | Anti-Tamper                | TEMPEST                                                              | TRANSEC                                         | Cover & Deception |
| <b>SML1</b> | 40+ bits symmetric key length, 80+ exponent 512+ modulus public key length   | SMI Cat X of [NSF98], 80+ exponent 512+ modulus public key length, 80+ hash key length    | comparable to [5200.1-R] | [FIP140] level 1 or 2      | comply with applicable EMI/EMC FCC standards or portions of [NT1/92] | low power unit                                  | TBD               |
| <b>SML2</b> | 80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length | SMI Cat Y of [NSF98], 160+ exponent 1024+ modulus public key length, 160+ hash key length | comparable to [5200.1-R] | [FIP140] level 3 or 4      | [NT1/92]                                                             | commercial spread spectrum signal techniques    | TBD               |
| <b>SML3</b> | Due to the complicated nature of this level, please consult with a NSA ISSE. | SMI Cat Z of [NSF98], also consult with a NSA ISSE.                                       | comparable to [5200.1-R] | [FIP140] level 4 or better | [NT1/92]                                                             | cryptographic spread spectrum signal techniques | TBD               |

# Confidentiality Mechanisms

|             | Cryptographic Algorithm                                                      |                                                                                           | Physical Security        | Technical Security         |                                                                      | Anonymity                                       |                   |
|-------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|--------------------------|----------------------------|----------------------------------------------------------------------|-------------------------------------------------|-------------------|
|             | Effective Key Length                                                         | Key Management                                                                            |                          | Anti-Tamper                | TEMPEST                                                              | TRANSEC                                         | Cover & Deception |
| <b>SML1</b> | 40+ bits symmetric key length, 80+ exponent 512+ modulus public key length   | SMI Cat X of [NSF98], 80+ exponent 512+ modulus public key length, 80+ hash key length    | comparable to [5200.1-R] | [FIP140] level 1 or 2      | comply with applicable EMI/EMC FCC standards or portions of [NT1/92] | low power unit                                  | TBD               |
| <b>SML2</b> | 80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length | SMI Cat Y of [NSF98], 160+ exponent 1024+ modulus public key length, 160+ hash key length | comparable to [5200.1-R] | [FIP140] level 3 or 4      | [NT1/92]                                                             | commercial spread spectrum signal techniques    | TBD               |
| <b>SML3</b> | Due to the complicated nature of this level, please consult with a NSA ISSE. | SMI Cat Z of [NSF98], also consult with a NSA ISSE.                                       | comparable to [5200.1-R] | [FIP140] level 4 or better | [NT1/92]                                                             | cryptographic spread spectrum signal techniques | TBD               |

# Integrity Mechanisms

|             | Cryptographic Algorithm                                                               |                                                                                                       | Physical Security              | Signature Checksum                                                      | Redundancy                                       |
|-------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------|-------------------------------------------------------------------------|--------------------------------------------------|
|             | Effective Key Length                                                                  | Key Management                                                                                        |                                |                                                                         |                                                  |
| <b>SML1</b> | 40+ bits symmetric key length,<br>80+ exponent<br>512+ modulus<br>public key length   | SML Cat. X of [NSF98],<br>80+ exponent 512+<br>modulus public key<br>length, 80+ hash key<br>length   | comparable<br>to<br>[5200.1-R] | parity, or commercial checksum, hash and, signature with SML1 algorithm | not applicable                                   |
| <b>SML2</b> | 80+ bits symmetric key length,<br>160+ exponent<br>1024+ modulus<br>public key length | SML Cat Y of [NSF98],<br>160+ exponent 1024+<br>modulus public key<br>length, 160+ hash key<br>length | comparable<br>to<br>[5200.1-R] | cryptographic checksum, hash, and signature with SML2 algorithm         | redundant data path with 100% correct comparison |
| <b>SML3</b> | Due to the complicated nature of this level, please consult with an NSA ISSE.         | SML Cat Z of [NSF98], also consult with an NSA ISSE.                                                  | comparable<br>to<br>[5200.1-R] | cryptographic checksum, hash and signature with SML3 algorithm          | multiple data paths with 100% correct comparison |

# Integrity Mechanisms

|             | Cryptographic Algorithm                                                               |                                                                                                       | Physical Security              | Signature Checksum                                                      | Redundancy                                       |
|-------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------|-------------------------------------------------------------------------|--------------------------------------------------|
|             | Effective Key Length                                                                  | Key Management                                                                                        |                                |                                                                         |                                                  |
| <b>SML1</b> | 40+ bits symmetric key length,<br>80+ exponent<br>512+ modulus<br>public key length   | SML Cat. X of [NSF98],<br>80+ exponent 512+<br>modulus public key<br>length, 80+ hash key<br>length   | comparable<br>to<br>[5200.1-R] | parity, or commercial checksum, hash and, signature with SML1 algorithm | not applicable                                   |
| <b>SML2</b> | 80+ bits symmetric key length,<br>160+ exponent<br>1024+ modulus<br>public key length | SML Cat Y of [NSF98],<br>160+ exponent 1024+<br>modulus public key<br>length, 160+ hash key<br>length | comparable<br>to<br>[5200.1-R] | cryptographic checksum, hash, and signature with SML2 algorithm         | redundant data path with 100% correct comparison |
| <b>SML3</b> | Due to the complicated nature of this level, please consult with an NSA ISSE.         | SML Cat Z of [NSF98], also consult with an NSA ISSE.                                                  | comparable<br>to<br>[5200.1-R] | cryptographic checksum, hash and signature with SML3 algorithm          | multiple data paths with 100% correct comparison |

# Availability Mechanisms

|             | TRANSEC                                                  | Anti-Tamper                       | Physical Security           | Redundancy                                     | Data Recovery                                                  |
|-------------|----------------------------------------------------------|-----------------------------------|-----------------------------|------------------------------------------------|----------------------------------------------------------------|
| <b>SML1</b> | high power                                               | [FIPS140]<br>level 1 or 2         | comparable<br>to [5200.1-R] | bypass<br>channel<br>available                 | informal<br>archival plan,<br>user backs up<br>own key or data |
| <b>SML2</b> | commercial<br>spread<br>spectrum signal<br>techniques    | [FIPS140]<br>level 3 or 4         | comparable<br>to [5200.1-R] | backup data<br>path, hot<br>spare              | formal archival<br>plan, central<br>back- ups                  |
| <b>SML3</b> | Cryptographic<br>spread<br>spectrum signal<br>techniques | [FIPS140]<br>level 4 or<br>better | comparable<br>to [5200.1-R] | multiple data<br>paths, multiple<br>hot spares | formal archival<br>plan, central,<br>offsite<br>back-ups       |

# Availability Mechanisms

|             | TRANSEC                                                  | Anti-Tamper                       | Physical Security           | Redundancy                                     | Data Recovery                                                  |
|-------------|----------------------------------------------------------|-----------------------------------|-----------------------------|------------------------------------------------|----------------------------------------------------------------|
| <b>SML1</b> | high power                                               | [FIPS140]<br>level 1 or 2         | comparable<br>to [5200.1-R] | bypass<br>channel<br>available                 | informal archival<br>plan, user backs<br>up own key or<br>data |
| <b>SML2</b> | commercial<br>spread<br>spectrum signal<br>techniques    | [FIPS140]<br>level 3 or 4         | comparable<br>to [5200.1-R] | backup data<br>path, hot<br>spare              | formal archival<br>plan, central<br>back- ups                  |
| <b>SML3</b> | Cryptographic<br>spread<br>spectrum signal<br>techniques | [FIPS140]<br>level 4 or<br>better | comparable<br>to [5200.1-R] | multiple data<br>paths, multiple<br>hot spares | formal archival<br>plan, central,<br>offsite<br>back-ups       |

# Security Management Mechanisms

|             | <b>Compromise Recovery</b>                  | <b>System Administration</b>                | <b>Training</b>                        | <b>OPSEC</b>                                      | <b>Trusted Distribution</b>                         | <b>Secure Operations</b>           | <b>Mechanism Management</b>              |
|-------------|---------------------------------------------|---------------------------------------------|----------------------------------------|---------------------------------------------------|-----------------------------------------------------|------------------------------------|------------------------------------------|
| <b>SML1</b> | Informal plan                               | See NSF98 for non-technical countermeasures | Training available at user discretion  | Implement at user's discretion                    | Direct vendor purchase                              | Informal plan of operation         | Procedural, user's discretion            |
| <b>SML2</b> | Detailed plan that is reviewed and approved | See NSF98 for non-technical countermeasures | Formal training plan                   | Training required, implement at user's discretion | Certificate of authenticity, virus scan, validation | Formal plan of operation           | Procedural, reminders, user's discretion |
| <b>SML3</b> | Detailed plan that is reviewed and approved | See NSF98 for non-technical countermeasures | Knowledge/skill certification required | Training required, implementation required        | Protective packaging, checksums, validation suite   | Detailed, formal plan of operation | Automated support                        |

# Security Management Mechanisms

|             | Compromise Recovery                         | System Administration                       | Training                               | OPSEC                                             | Trusted Distribution                                | Secure Operations                  | Mechanism Management                     |
|-------------|---------------------------------------------|---------------------------------------------|----------------------------------------|---------------------------------------------------|-----------------------------------------------------|------------------------------------|------------------------------------------|
| <b>SML1</b> | Informal plan                               | See NSF98 for non-technical countermeasures | Training available at user discretion  | Implement at user's discretion                    | Direct vendor purchase                              | Informal plan of operation         | Procedural, user's discretion            |
| <b>SML2</b> | Detailed plan that is reviewed and approved | See NSF98 for non-technical countermeasures | Formal training plan                   | Training required, implement at user's discretion | Certificate of authenticity, virus scan, validation | Formal plan of operation           | Procedural, reminders, user's discretion |
| <b>SML3</b> | Detailed plan that is reviewed and approved | See NSF98 for non-technical countermeasures | Knowledge/skill certification required | Training required, implementation required        | Protective packaging, checksums, validation suite   | Detailed, formal plan of operation | Automated support                        |

# Assurance Level

---

---

- Table points to EAL5  
semi-formally designed and tested

# Assess Residual Risk

---

---

- Having a lower assurance level may allow an undiscovered vulnerability to exist which a sophisticated adversary could exploit to pre-place malicious code in anticipation of a crisis.
- Inadvertent flooding by legitimate users could deny service to the Secret network.

# Summary

---

---

- Can we meet the desired security policy with the selected security mechanisms?
- Is the residual risk acceptable?
- The strategy was useful in selecting security mechanisms that are *good enough*.
- The next step in the development process would be to define requirements.

# Questions?



# Backup Slides



# I&A Mechanisms

|                  | System IDs (SIDs)                                                     | Biometrics                             | Passwords<br>PINs<br>Challenge/<br>Response | Tokens                              | Certificates                        | Crypto-<br>graphic<br>Algorithm | Personnel<br>Security              |
|------------------|-----------------------------------------------------------------------|----------------------------------------|---------------------------------------------|-------------------------------------|-------------------------------------|---------------------------------|------------------------------------|
| <b>SML<br/>1</b> | uniqueness                                                            | not applicable                         | have one                                    | badge/key static                    | bind w/SML1 cryptographic algorithm | See Confidentiality Mechanisms  | commercial hiring practices        |
| <b>SML<br/>2</b> | uniqueness and minimum character length                               | use one Biometric                      | minimum effective length – TBD              | memory device, updated periodically | bind w/SML2 cryptographic algorithm |                                 | equivalent of SECRET clearance     |
| <b>SML<br/>3</b> | uniqueness, minimum character length, minimum distance(e.g., Hamming) | use one Biometric with a liveness test | minimum effective length - TBD              | CIK, updated every time             | bind w/SML3 cryptographic algorithm |                                 | equivalent of TOP SECRET clearance |

# Access Control Mechanisms

|             | <b>Anti-Tamper</b>          | <b>Mandatory Access Control</b>                                                   | <b>Discretionary Access Control</b> | <b>Certificates</b>                 | <b>Personnel Security</b>          |
|-------------|-----------------------------|-----------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|------------------------------------|
| <b>SML1</b> | [FIPS140] level 1 or 2      | not applicable                                                                    | comparable to Unix permission bits  | bind w/SML1 cryptographic algorithm | commercial hiring practices        |
| <b>SML2</b> | [FIPS140] level 3 or 4      | labels bound to data having integrity and binding function both at the SML2 level | access control lists (ACLs)         | bind w/SML2 cryptographic algorithm | equivalent of SECRET clearance     |
| <b>SML3</b> | [FIPS140] level 4 or better | labels bound to data having integrity and binding function both at the SML3 level | access control lists (ACLs)         | bind w/SML3 cryptographic algorithm | equivalent of TOP SECRET clearance |

# Accountability Mechanisms

|             | <b>Audit</b>                      | <b>Intrusion Detection</b>                              | <b>Identification and Authentication</b> |
|-------------|-----------------------------------|---------------------------------------------------------|------------------------------------------|
| <b>SML1</b> | informal reaction mechanism       | static system with informal reaction mechanism          | see I&A table for SML1                   |
| <b>SML2</b> | formal reaction plan and strategy | dynamic system with formal reaction mechanism           | see I&A table for SML2                   |
| <b>SML3</b> | formal reaction plan and strategy | dynamic, adaptive system with formal reaction mechanism | see I&A table for SML3                   |

# Non-Repudiation Mechanisms

|             | <b>Signature</b>                       | <b>Trusted Third Party</b>                | <b>Accountability</b>             | <b>I&amp;A</b>         | <b>Archive</b>                                        |
|-------------|----------------------------------------|-------------------------------------------|-----------------------------------|------------------------|-------------------------------------------------------|
| <b>SML1</b> | sign with SML1 cryptographic algorithm | see I&A Table for SML1 Personnel Security | see Accountability table for SML1 | see I&A table for SML1 | informal archival plan, user backs up own key or data |
| <b>SML2</b> | sign with SML2 cryptographic algorithm | see I&A Table for SML2 Personnel Security | see Accountability table for SML2 | see I&A table for SML2 | formal archival plan, central back-ups                |
| <b>SML3</b> | sign with SML3 cryptographic algorithm | see I&A Table for SML3 Personnel Security | see Accountability table for SML3 | see I&A table for SML3 | formal archival plan, central, offsite back-ups       |