Multi-Tier Security Profiles

Briefing to ISPAB

David L. Jarrell

FTS Office of Service Development

March 13, 2003

Multi Tier Security Profiles (MTSP)

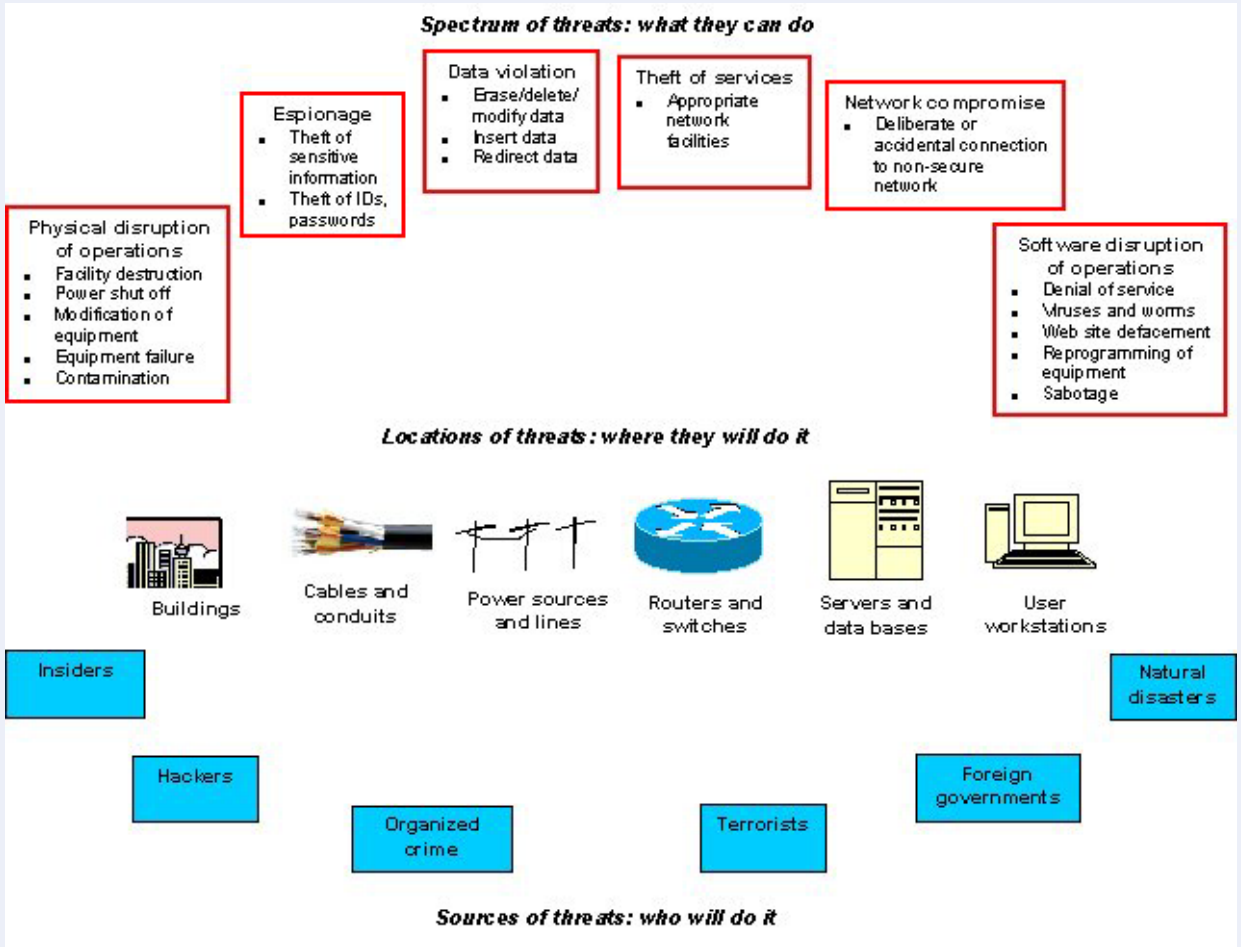
This briefing is to provide the ISPAB with an update on how GSA-FTS is addressing the requirement to increase security in the services being delivered to their customer agencies.

Briefing Outline

- Threat Summary
- FTS Security Enhancement Program
- What is MTSP?
- Benefits of MTSP to Information Assurance
- Program Status and Next Steps

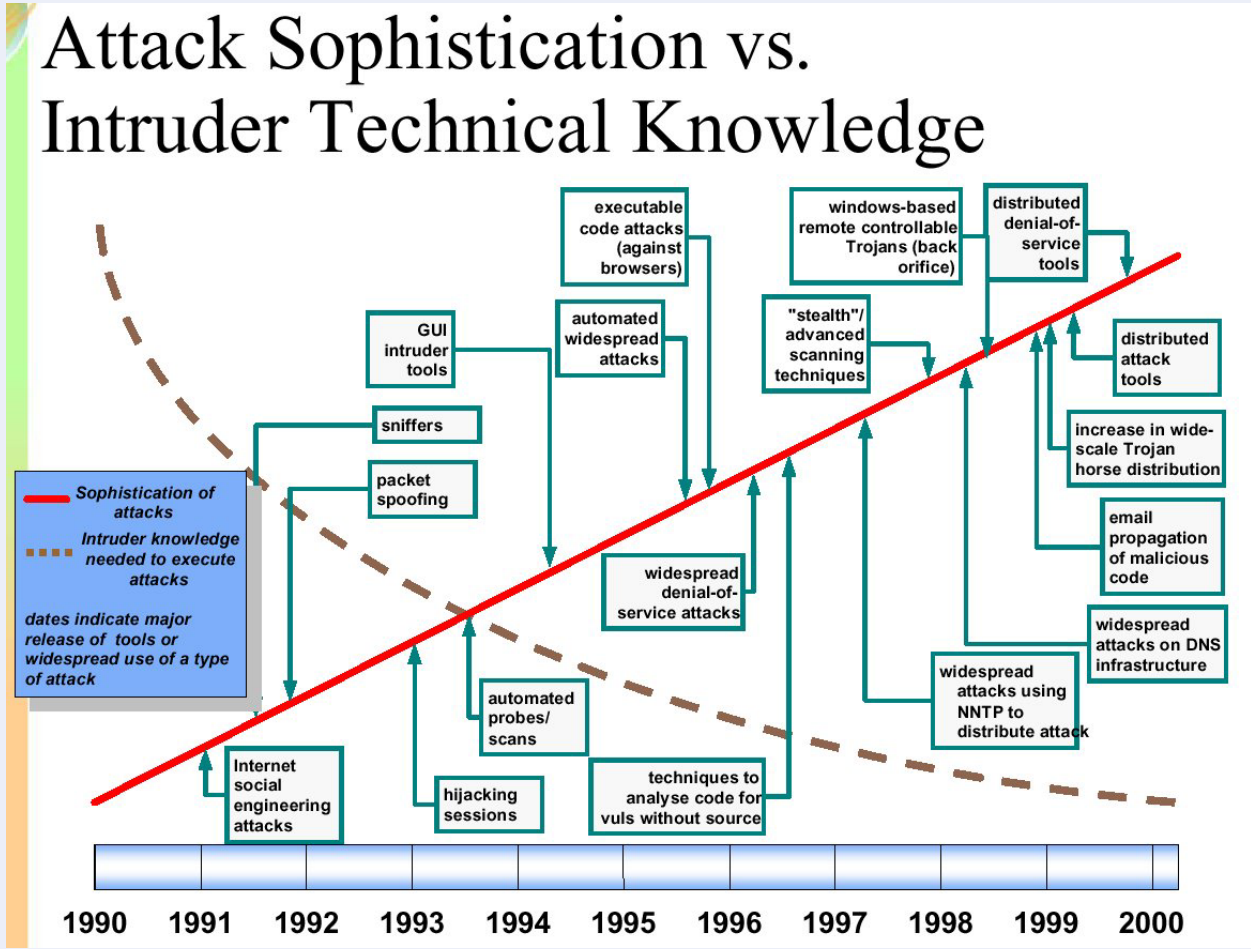
Threat Summary

- Continuing Proliferation of Threats
- Attacks becoming more frequent and sophisticated
- Targeted at infrastructure as well as desktop
- Results in loss of productivity, compromised data, financial impact
- Incidents / Attacks may be intentional or unintentional



Attacks Maturing and Easier to Execute

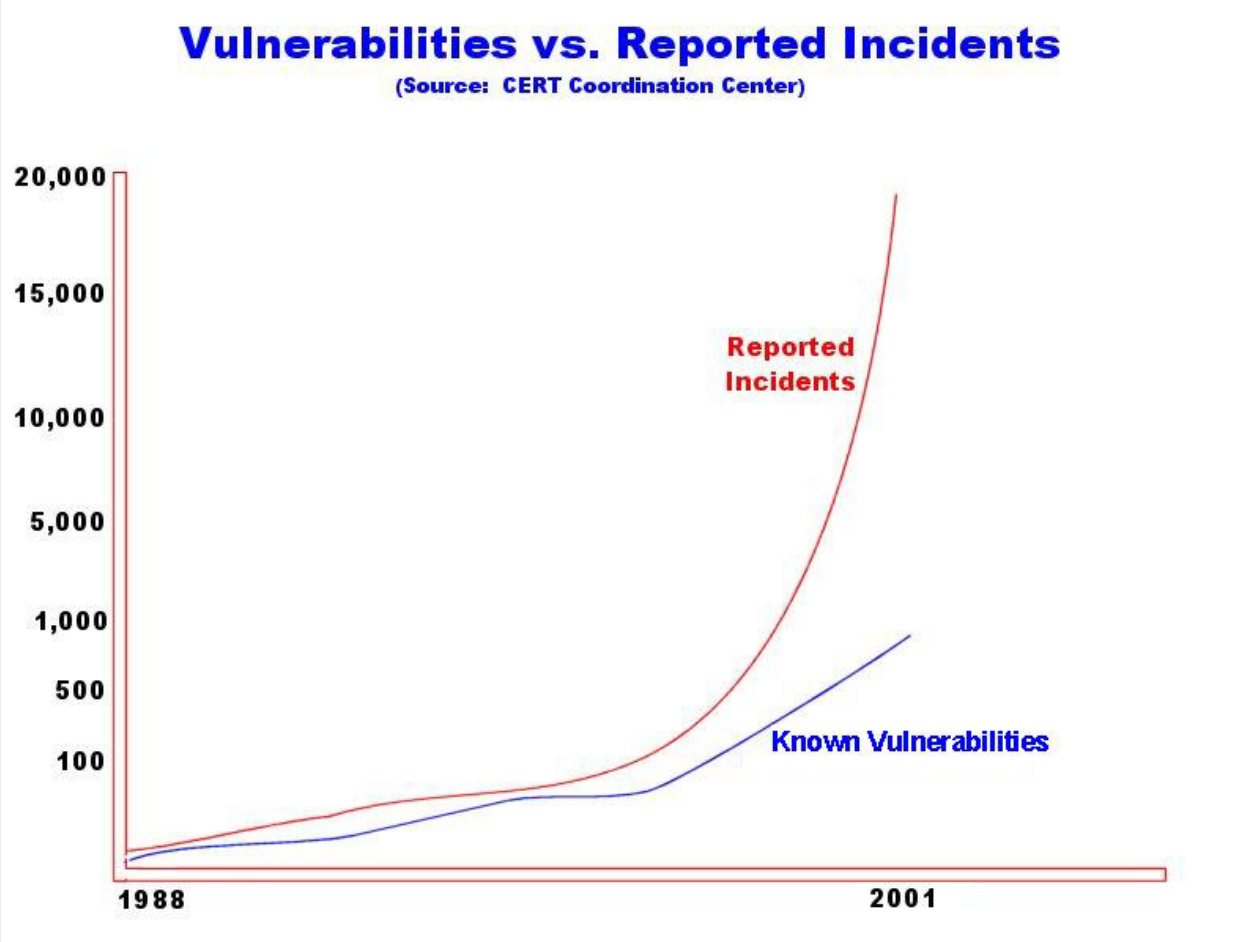
- Exploits and attacks are easier for the novice computer user to perpetrate, e.g:
  - Network Mapping
  - Port Scanners
  - DOS/DDOS
  - Social Engineering
  - Password cracking scripts
  - Viruses
  - Trojans
  - Worms



Source: Carnegie Mellon CERT/CC

Vulnerabilities and Incidents Increasing

- New vulnerabilities coupled with ease of execution resulting in exponential growth in incidents
- More effective incident reporting requirements for network attacks, intrusion, and viruses.
- 75-80% of incidents go unreported
- Top 10 Vulnerabilities ~ old wine/new bottles e.g., Insecure Defaults



FTS Security Enhancement Philosophy

- Years of "talking" about network vulnerabilities have done little to create an effective defense strategy.
- FTS Office of Service Development plan integrates security features into existing telecommunications service offerings
- Goal - Enhance IT services with the security technologies, policies, and procedures appropriate for all levels of mission sensitivity and criticality
- Solutions satisfy IT and telecommunications needs while improving the overall security profile of our customers.
- Results – "Added Value" to improve security, reliability, and survivability for resources of the Federal Information Infrastructure.

FTS Security Enhancement Program

…… is a comprehensive developmental initiative to bundle a wide range of security features and services that satisfy the diverse and complex government needs. This "IT Security Enhancement Program" as conceived, includes offerings to address technical, administrative and physical security requirements.

MTSP
for securing the IT infrastructure
FTS 2001, MAA

→ Tier 1- Standard
Tier 2 – Protected
Tier 3 – High Assurance
Tier 4 – Network High

Co-managed Network Services
Safeguard

→ Network Administration
Intrusion Detection
Incident Reporting & Response

IT Integration
for assessment and interoperability
Safeguard, Millennia Lite

→ Risk Assessment
Security Compliance/Oversight
Interoperability Testing

Secure Wireless
connectivity to Infrastructure
FTS 2001, MAA, FedWireless

→ Wireless Networking
Pt. to Pt. Microwave
Free Space Optics
Wireless Messaging

Security Testing and Evaluation
Safeguard, Millennia Lite

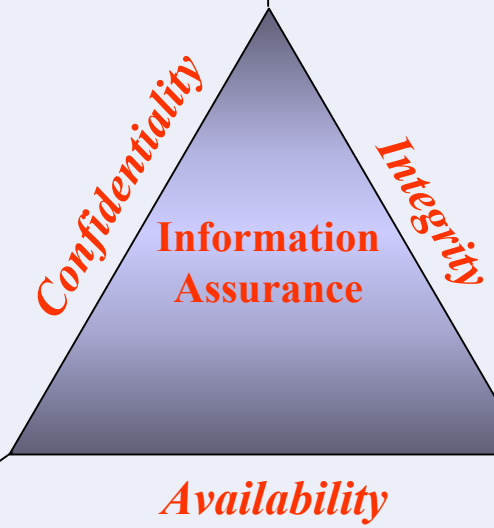
→ Penetration Tests
Vulnerability Analysis
Policy Evaluation
Certification & Accreditation

Security Policy Development and Training
Safeguard

→ Risk Management
Physical
Administrative
Technical
Threat Awareness & Security Testing

Security Service Component Value

- Secure Web Proxy
- Firewalls
- Intrusion Detection
- Packet Filtering
- VPN
- Trusted Gateway
- Secure Mail Guard
- Network Isolation
- Vulnerability Analysis
- Compliance Testing
- Certification and Accreditation



- Personnel Reliability Requirements
- Network Management
- Incident Reporting and Response
- Configuration Management
- VPN
- Trusted Gateway
- Anti-Virus
- Secure Mail Guard
- Certification and Accreditation

- 99.8% upgradeable to '5 nines' service availability as required
- Risk Management
- Cross Domain Interoperability
- 24x7 Help Desk

Office of Service Development

"Never lose sight of the big picture."

Mechanisms to Provide Security Services

- Past Approaches
  - Security services as add-ons to existing contracts
    - VPNs, Firewalls, Managed Services
    - Disaster recovery solutions
- FTS Approach
  - Address security shortfalls as identified by GAO, NSTAC, FedCIRC, SANS, etc.
  - Create Telecommunication Service offerings with embedded security features in concert with a subscribing agency's mission criticality and information sensitivity
  - Modification of existing FTS contracts (e.g., FTS2001, MAA, Millennia……others) and new contracts as necessary to address government needs
- Desired Outcomes
  - Significantly improve the overall security profile of the Federal Information Infrastructure
  - Improve the attractiveness, affordability and effectiveness of FTS IT & telecom services

Ingredients for Success

For success, Information Assurance must be actionable and measurable

- People
  - Assign responsibility and accountability
  - Train, reinforce and test the skills needed to address the problem
  - Instill awareness and provide job aides for EVERYONE
  - Recognize, reward and reinforce positive behavior
- Process
  - Assess mission needs and associated risks to determine protection needs
  - Select and implement policies and controls to meet those needs
  - Identify Performance Measurement criteria
  - Implement a program of routine tests and examinations for evaluating policy and security feature effectiveness … and make changes as needed
- Technology
  - There are no "silver bullet" solutions
  - Build architectures suited to the enterprise … business friendly but effective
  - Bolt-on solutions are costly, sometimes ineffective and difficult to implement
  - Include security in the systems development and selection lifecycle

MTSP Conceptual Tier Architectures

Tier 1 – *Standard*

Non-mission critical

Non-sensitive information

Tier 2 – *Protected*

Sensitive but Unclassified (SBU)

Connectivity with High Assurance technologies

Tier 3 – *High Assurance*

Appropriate for SBU or classified information up to SECRET

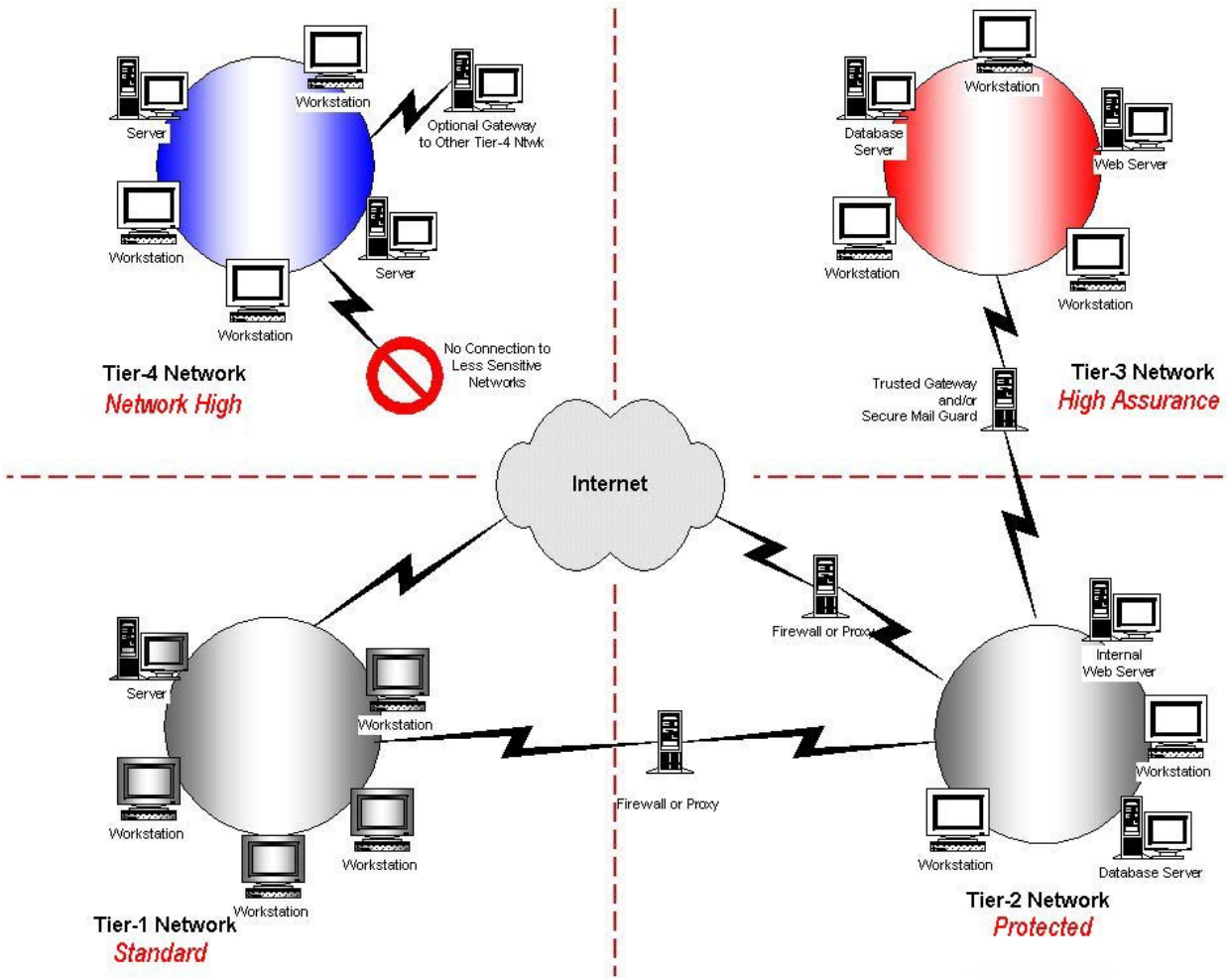
Connectivity to Tier 2 through Trusted Gateway, Secure Mail Guard, or S/W Proxy

Tier 4 – *Network High*

Appropriate for SBU or classified information up to TOP SECRET

Most Secure

No external connectivity



Office of Service Development

"Never lose sight of the big picture."

MTSP Assures Compliance

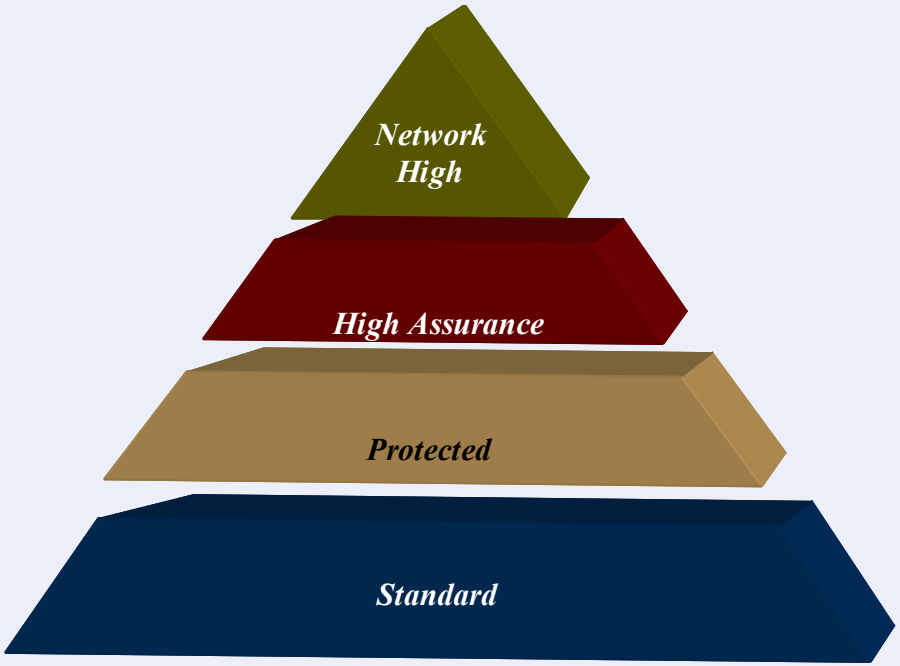
- Certification and Accreditation
  - OMB Circular A-130 Appendix III
    - Security of Federal Automated Information Systems
  - NIST 800-37
    - Guidelines for the Security Certification and Accreditation of Federal IT Systems
  - NSTISSI 1000
    - National Information Assurance Certification and Accreditation Process (NIACAP)

Advantage of Tiered Services

- MTSP addresses the fact that 'one size does not fit all' for the needs of non-military government agencies
- MTSP works to de-mystify and simplify the many choices of security services
- Provides Value and Cost Effectiveness
  - Evaluation and packaging of existing service alternatives
  - GSA-FTS has negotiated best value from vendors easing purchasing related bureaucracy for individual agencies and managers
  - Cost benefits of outsourcing IA extend through entire life-cycle

"The MTSP effort provides government clients with just the right range of different protection profiles. Varying degrees of threat combined with varying criticality of government assessments requires the type of tiered approach offered in MTSP."– *Dr. Edward Amoroso, VP of AT&T Security*

Security Enhancement Program Status



- Contract modifications for FTS 2001 and MAA currently underway
- MTSP Tier 1 Services available now
- MTSP Tiers 2 and 3 available 2QFY03
- MTSP Tier 4 service available 3QFY03
- Security Enhancement Program Next Steps
  - Develop Secure Wireless Services
    - Projected availability: July '03

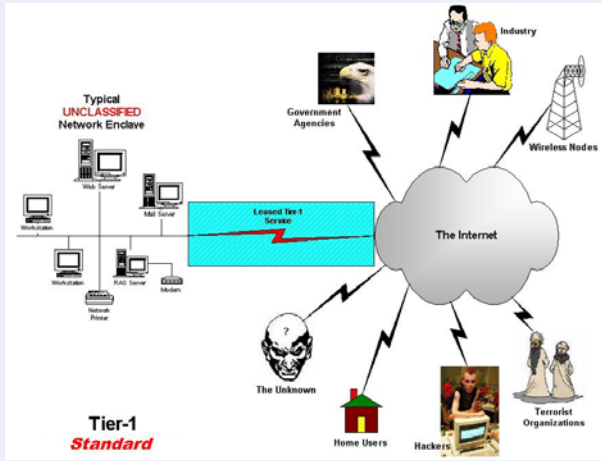
GSA

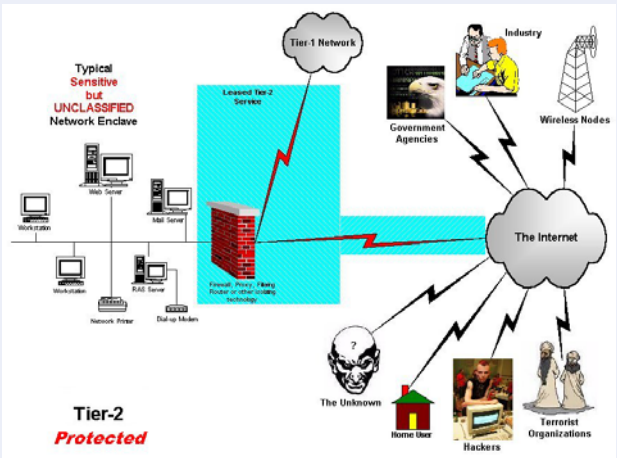
Questions?

Backup Slides

MTSP Service Offerings

- Tier 1 *Standard*
  - Service reliability > 99.8%
  - 24 x 7 Help Desk

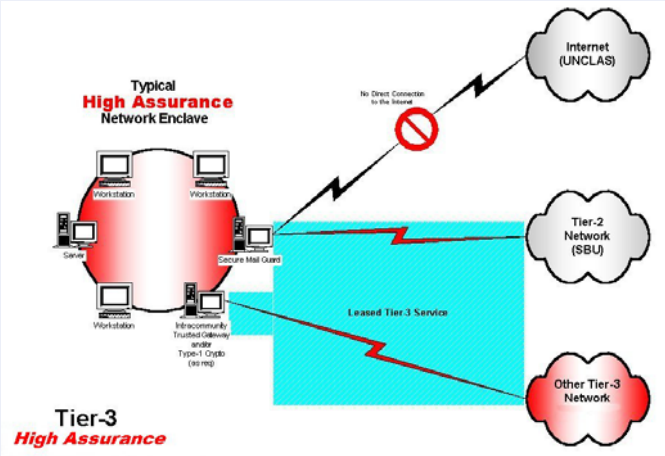


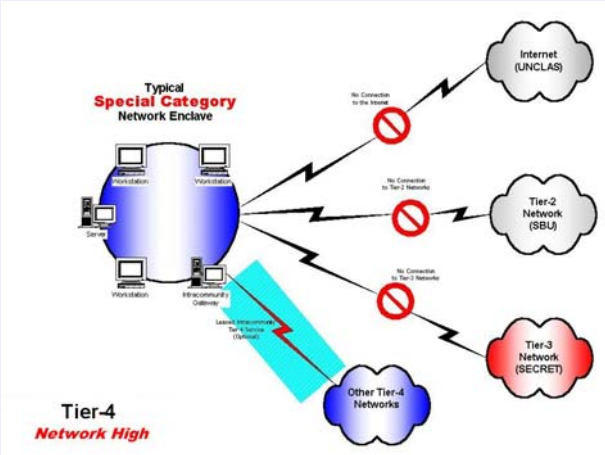


- Tier 2 *Protected*
  - Tier 1 services plus…
  - Firewall, IDS, Anti-Virus, Packet Filtering, VPN, Secure Web Proxy, CM, Remote and on-site Network Management

MTSP Service Offerings

- Tier 3 *High Assurance*
  - Tier 2 services plus…
  - Type 1 Encryption Capable, Trusted Gateway, Secure Mail Guard





- Tier 4 *Network High*
  - Isolated Network
  - Firewall, IDS, Packet Filtering, VPN, Type 1 Encryption Capable, CM, On-site Network Management

Next Steps under the FTS Security Enhancement Program

- Secure Wireless Solutions
  - Wireless Technology & Service Inventory
  - Vulnerability Assessment
  - Identify and package security solutions
- Policy Templates for
  - Physical
  - Administrative
  - Technical
- E-Gov Solution-based Services