



We Bring Security To Light™

# Briefing: Interceptor™ Optical Network Security System

G6/S6 Conference  
Tacoma, WA  
February 18, 2009

Joe Giovannini

# The SIPRNET Challenge

**NetworkIntegrity**  
SYSTEMS

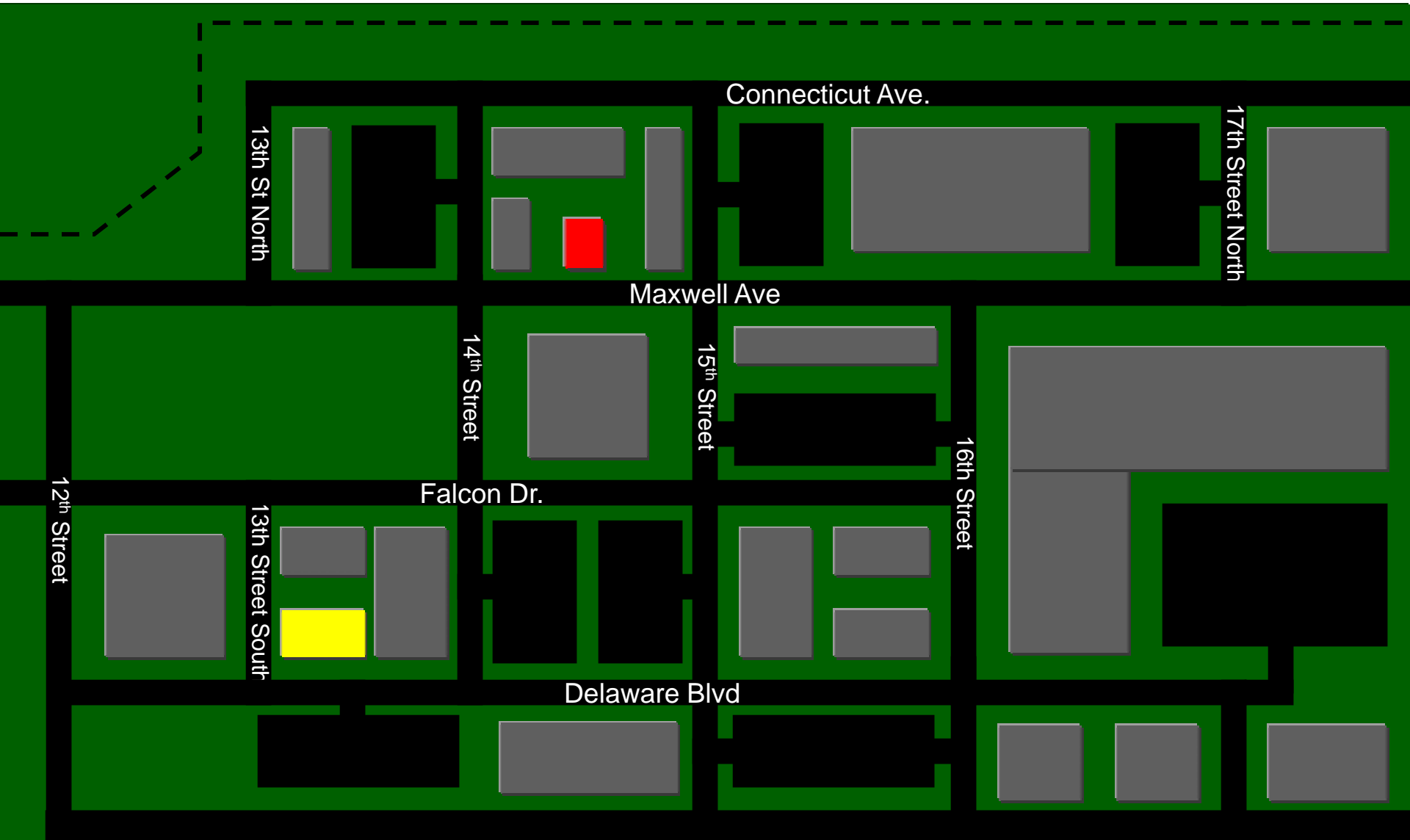
We Bring Security To Light™



**While Insuring the Confidentiality, Integrity and Availability of the Information**

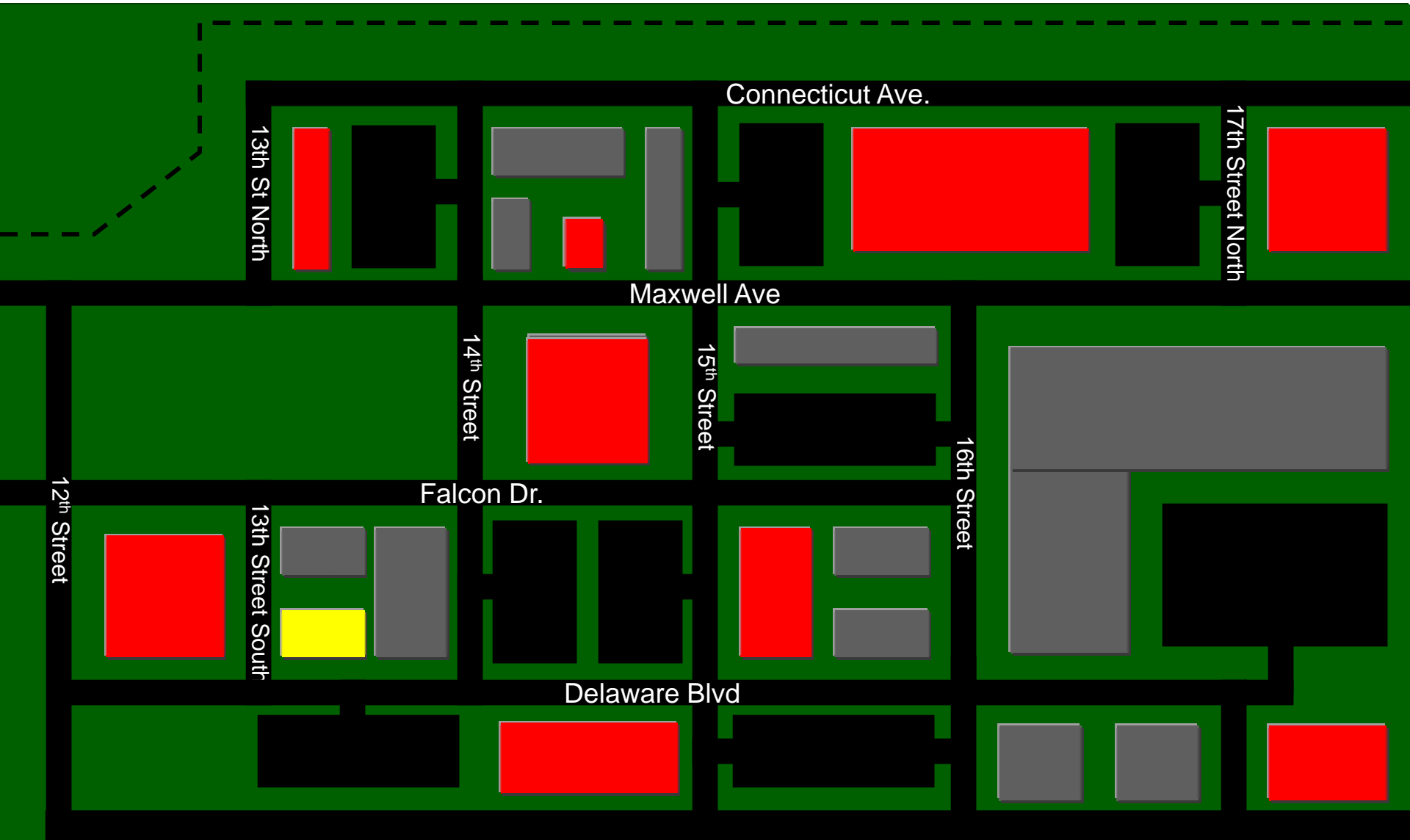
# The SIPRNET Challenge *Yesterday...*

*SIPRNET Required in Minimal Sites*



# The SIPRNET Challenge *Today...*

*SIPRNET Required at Many Sites*



# SIPRNET Security Options

Transmission of National Security Information must be protected by one of the following methods:

1. Encryption
2. Protected Distribution System (PDS)



Each method provides varying degrees of Information Assurance:

- Confidentiality
- Integrity
- Availability

# Protected Distribution System (PDS)

## NSTISSI 7003

- Differentiates requirements for transport of encrypted vs. unencrypted information
- Establishes PDS guidelines for Low, Medium and High Threat areas
- Provides alternatives for protection of unencrypted information:
  - Hardened Carrier System
  - Alarmed Carrier System
  - Continuously Viewed Carrier



We Bring Security To Light™



# Protected Distribution System (PDS)

Goal of ANY PDS is to maximize protection according to the three **D's**:

- **DETER** tampering with protected infrastructure
  - *Discourage "DITY" users & curiosity seekers*
- **DETECT** any unauthorized, malicious or surreptitious attempts to tamper with or access protected assets
  - *Through visual inspection or alarms*
- Maximize the **DIFFICULTY** - both in time to defeat and ability to conceal - of accessing protected assets
  - *Ensure ability to access takes longer than ability to detect and respond*



# Hardened PDS

- Provide physical protection of network infrastructure
- Deters intrusions and makes difficult
- Maintains full network bandwidth
- Requires Periodic Visual Inspections (PVI) - so must be visible
- Inability to be installed on pre-existing cables being upgraded to handle secure transmissions, for instance, SIPRNET tunneling applications.

***Outdoor: Concrete Encased Duct Bank***



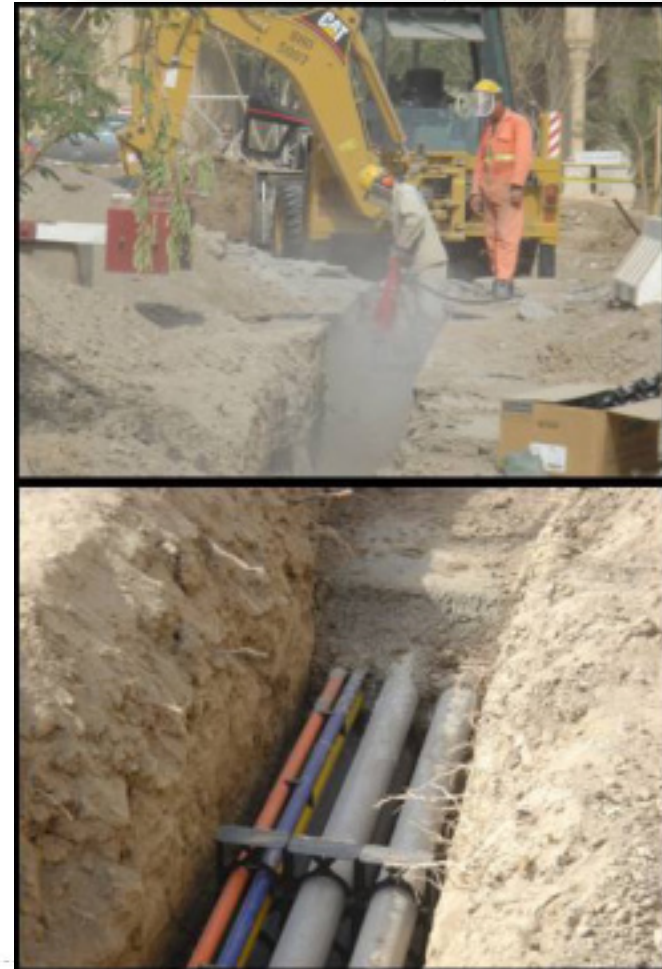
***Indoor: EMT, Rigid Metallic Conduit, Aesthetic Raceway***

# Alarmed Carrier OSP Network Deployment

- Use of alarmed carrier is being utilized more and more in-place of encryption or concrete encased duct banks for building-to-building connections to:
  - Reduce deployment costs
  - Alleviate lead times or delays in getting concrete delivered
  - Minimize the impact on base caused by disruptive construction activity
  - Accelerate deployments
  - Make use of existing cables
  - Minimize future environmental impact caused by buried concrete

**NetworkIntegrity**  
SYSTEMS

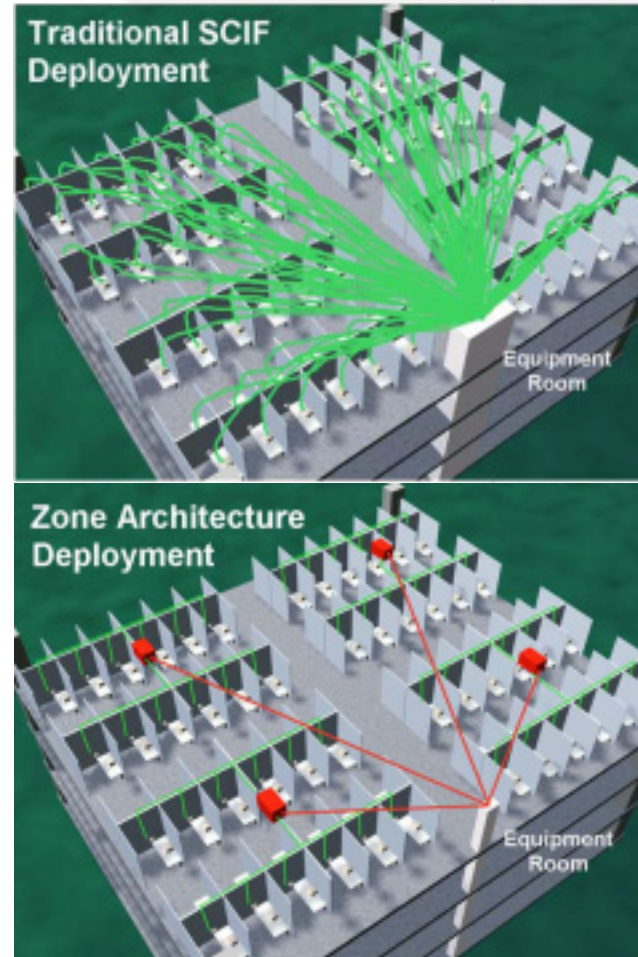
We Bring Security To Light™



# Alarmed Carrier

## Indoor Network Deployment

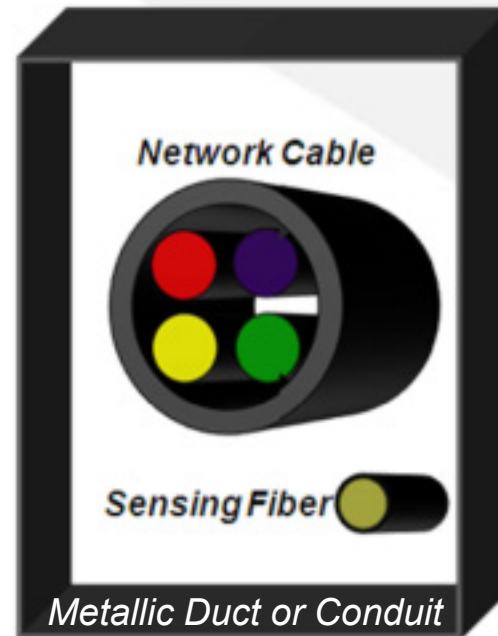
- Use of alarmed carrier is increasing because of these benefits:
  - Ability to install cables and carrier above ceiling
  - Eliminate aesthetic issues in newly constructed or renovated buildings (remove unsightly pipe from walls)
  - Reduce the impact of Periodic Visual Inspection requirements on personnel
  - Make use of existing cables
  - Minimize the impact on personnel caused by disruptive construction activity
  - Accelerate deployments
- Implementing alarmed carrier as part of a Zone Architecture allows the zone trunk cables (between the telecom closet and the zone box) to be installed above the ceiling



# Interceptor: Not a Traditional Alarm Carrier System

## Shortcomings of traditional alarm carrier:

- Traditional Alarmed Carriers morphed from perimeter security systems - not developed with data security in mind
- Traditional Alarmed Carrier monitors the *pathway* carrying the cables
- Requires a special sensing fiber
- No specificity to events: frequent false alarms - must be set very sensitive to detect intrusions into duct system
- Difficult to retrofit into existing cable systems when upgrading from unclassified to classified traffic



Traditional Alarm Carrier System

# Interceptor™ Optical Network Security System

Developed in part with DoD funding to monitor and protect the integrity and availability of C4ISR networks

- Monitors actual cables being protected to detect physical tampering or attempts to access them
- Learns network physical environment to eliminate false alarms
- Plug-and-Protect™ - setup in less than an hour
- 100% physical layer protection
  - *Does not touch or process data*
  - *Usually installed on dark or unused fibers but works on active fibers too*
  - *No impact on network bandwidth*
- Supports any network protocol - including 10GBase - and any fiber type (SM or MM)
- Interfaces with building security system through dry contact interface
  - Can also be monitored using SNMP traps, Ethernet

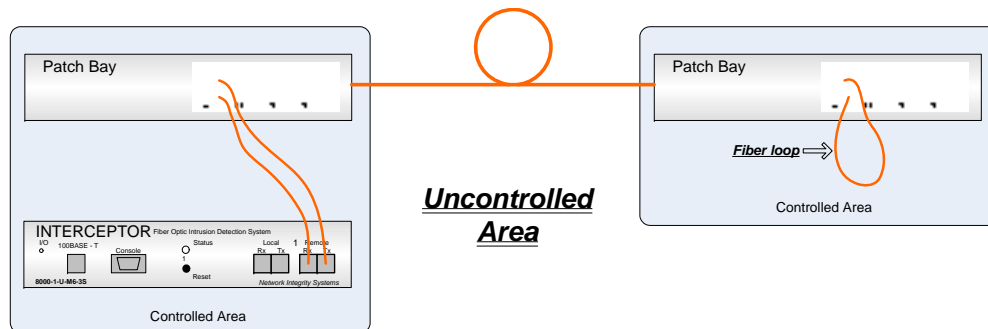


**NetworkIntegrity**  
SYSTEMS

We Bring Security To Light™

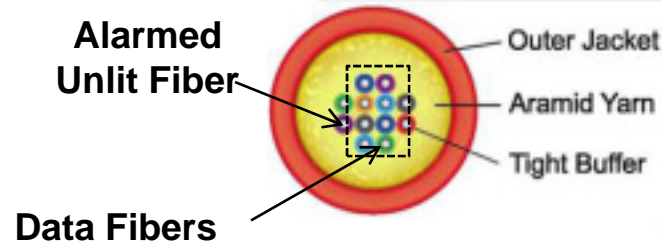
# How Interceptor Works

- Interceptor turns unused, unlit, spare fibers into an internal "sensor" along an entire cable run
- This sensitizes the entire cable structure to intrusion
- Interceptor is installed on one end of cable

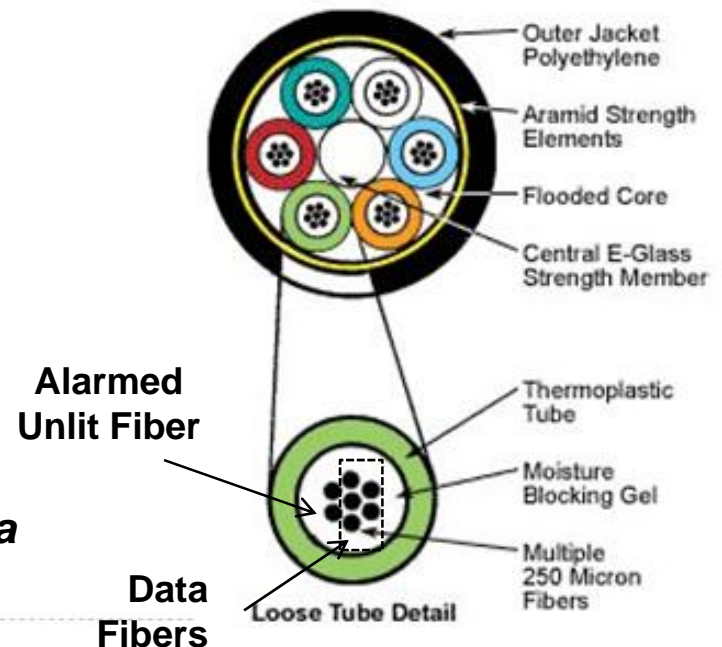


**Monitoring as few as two fibers protects up to a 144-fiber "loose tube" cable**

## INDOOR CABLE



## OUTDOOR CABLE



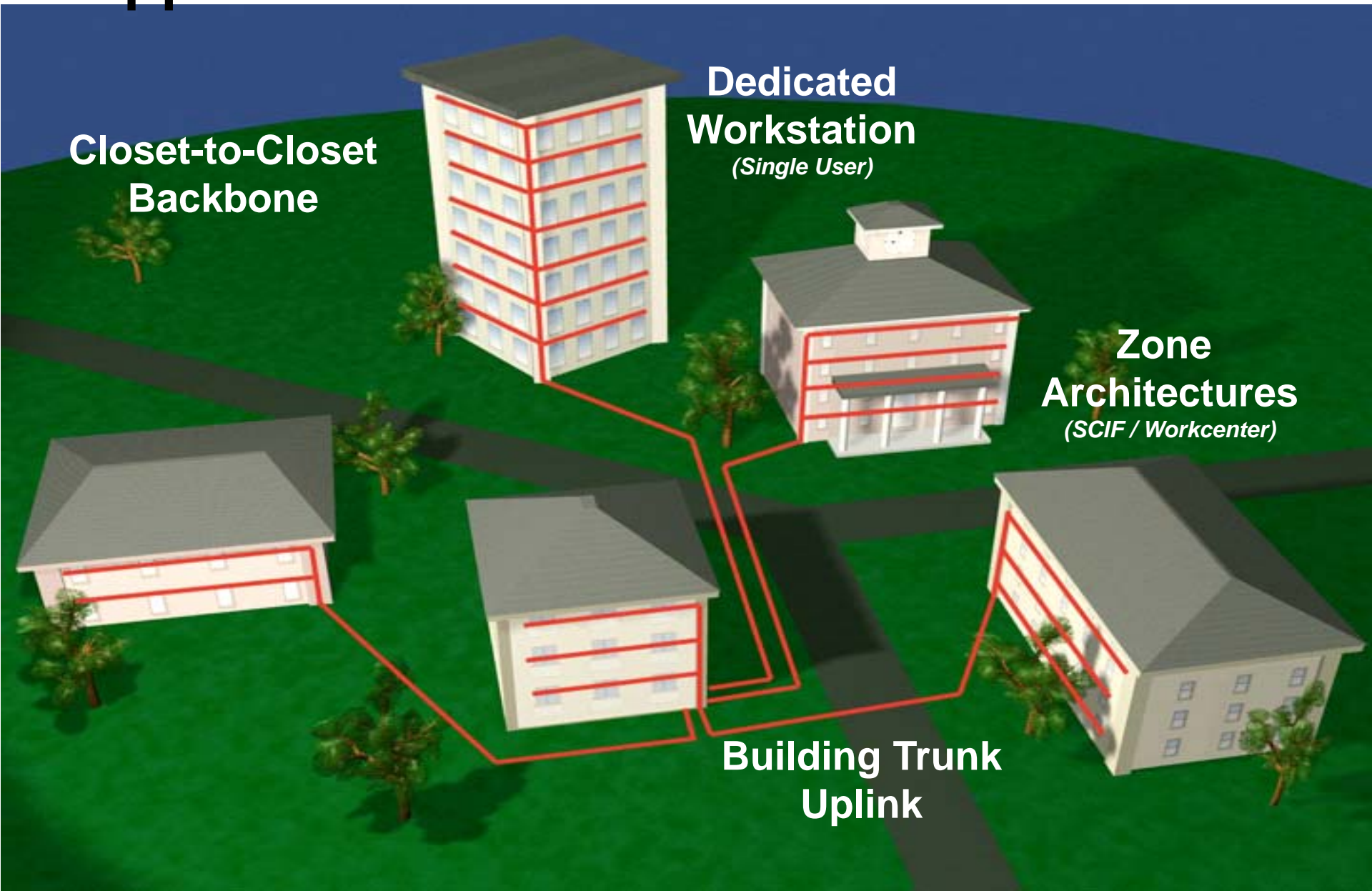
# Interceptor Works in a Variety of Applications

**Closet-to-Closet  
Backbone**

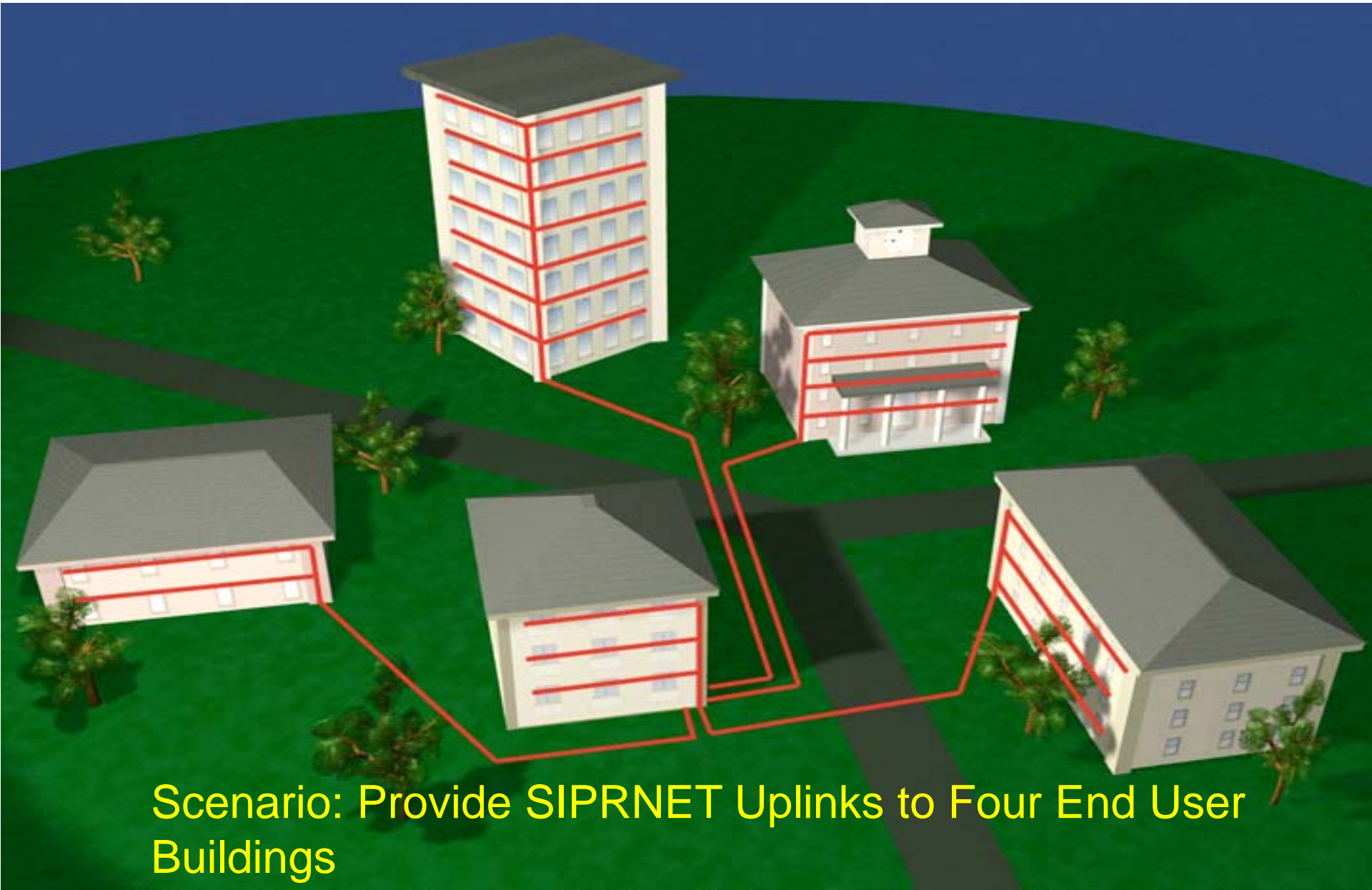
**Dedicated  
Workstation**  
*(Single User)*

**Zone  
Architectures**  
*(SCIF / Workcenter)*

**Building Trunk  
Uplink**



# Comparison of Encryption, Hardened PDS and Interceptor with respect to cost, scalability and bandwidth...



Scenario: Provide SIPRNET Uplinks to Four End User Buildings

# Encryption

## Deployment Outcome

Cost: **\$45,000**

Install Time: **1 Day**

Lead Time: **6-9 Months**

Bandwidth: **<100MB**

**Uplink: 25  
Mbps**

**User: <1  
Mbps**

**30 Users**

**2 Users**

**Uplink: 25  
Mbps**

**User: 12  
Mbps**

**6 Users**

**DISA  
POP**

**8 Users**

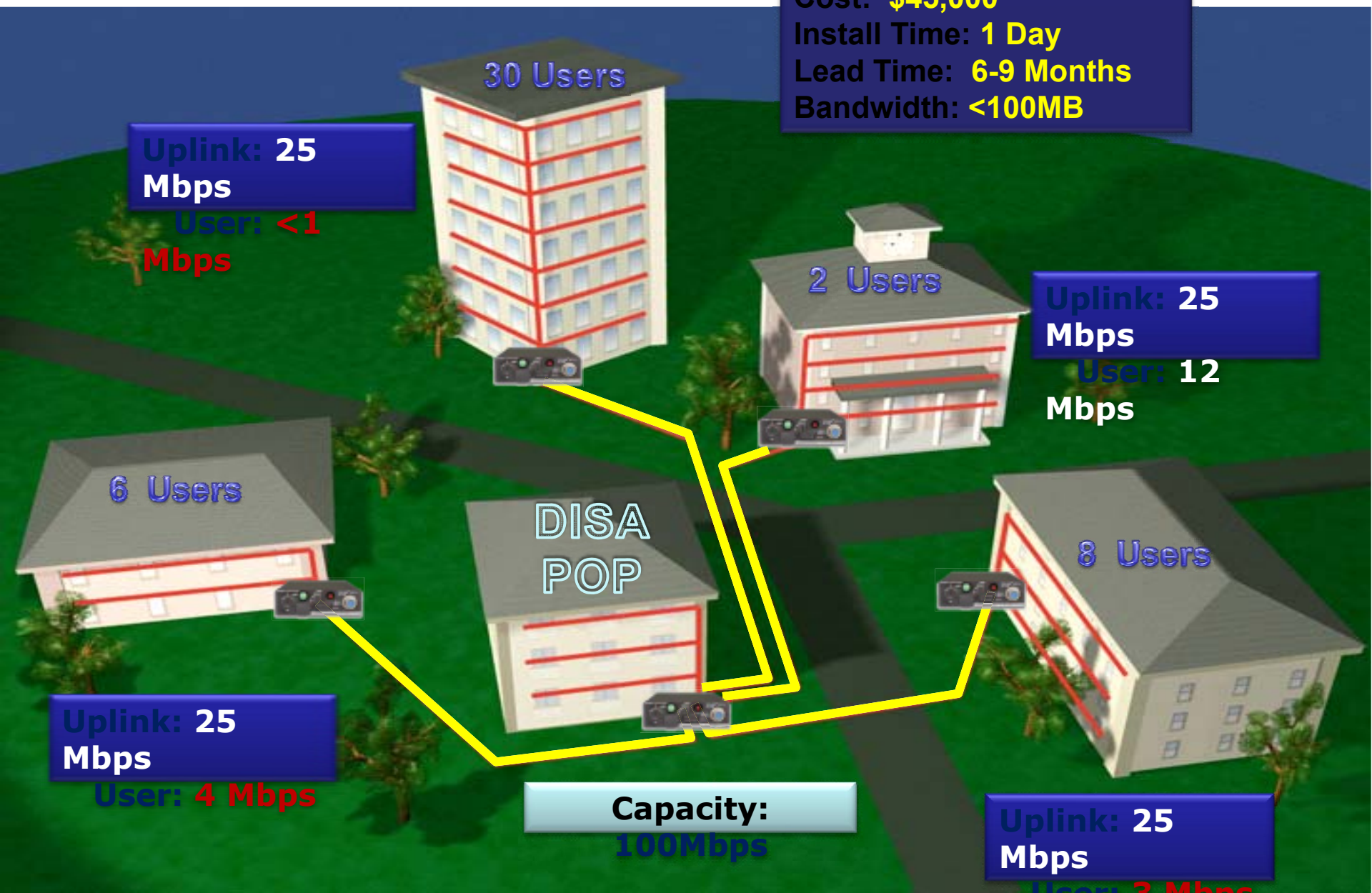
**Uplink: 25  
Mbps**

**User: 4 Mbps**

**Capacity:  
100Mbps**

**Uplink: 25  
Mbps**

**User: 3 Mbps**



# Hardened PDS

## Deployment Outcome

Cost: **\$800,000 x 4**

Install Time: **6-8 Weeks**

Lead Time: **~4 Weeks**

Bandwidth: **Unlimited**



Concrete-Encased  
Duct Bank

# Interceptor

A single Interceptor provides secure connectivity to all four buildings.

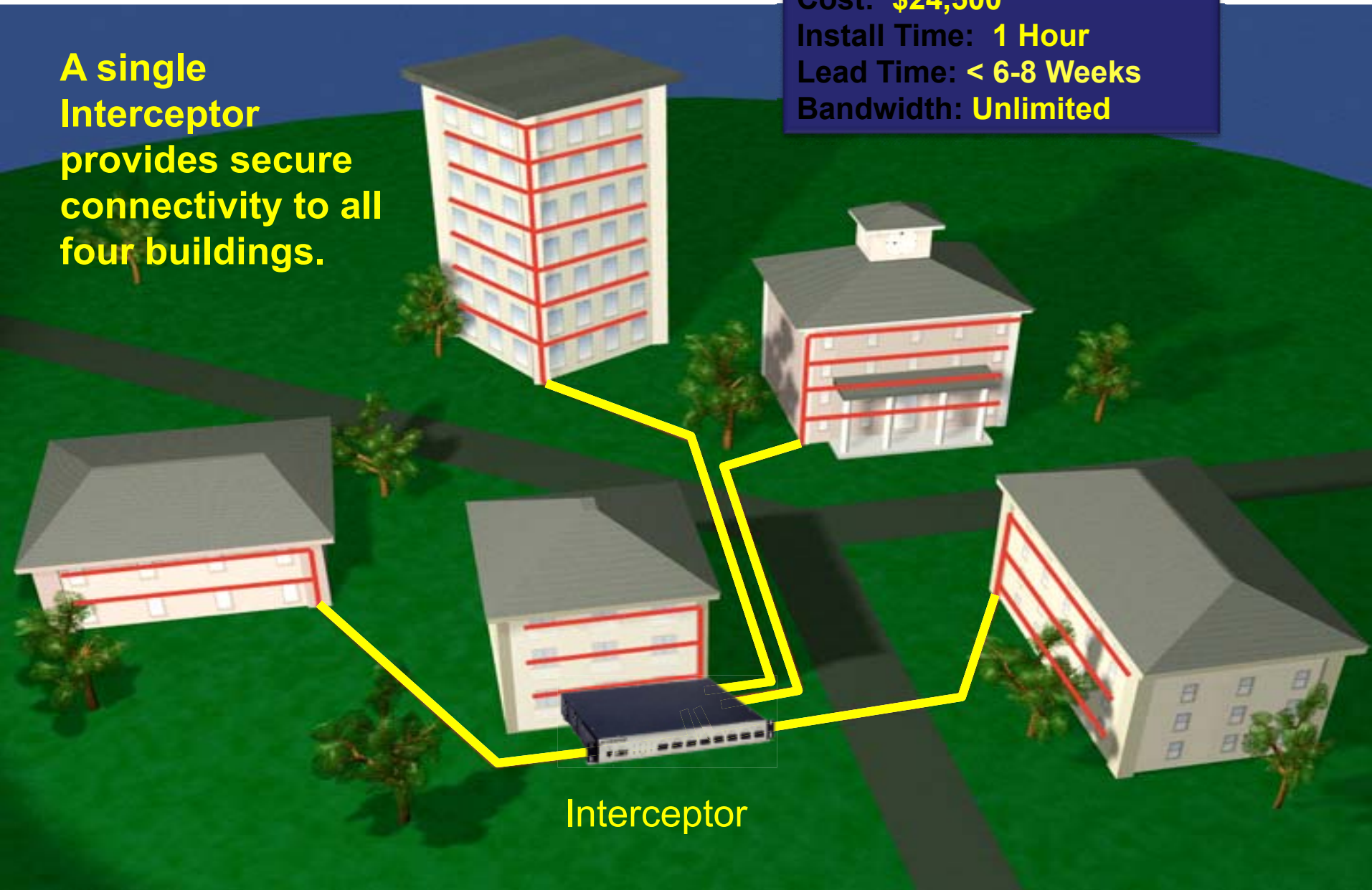
## Deployment Outcome

Cost: **\$24,500**

Install Time: **1 Hour**

Lead Time: **< 6-8 Weeks**

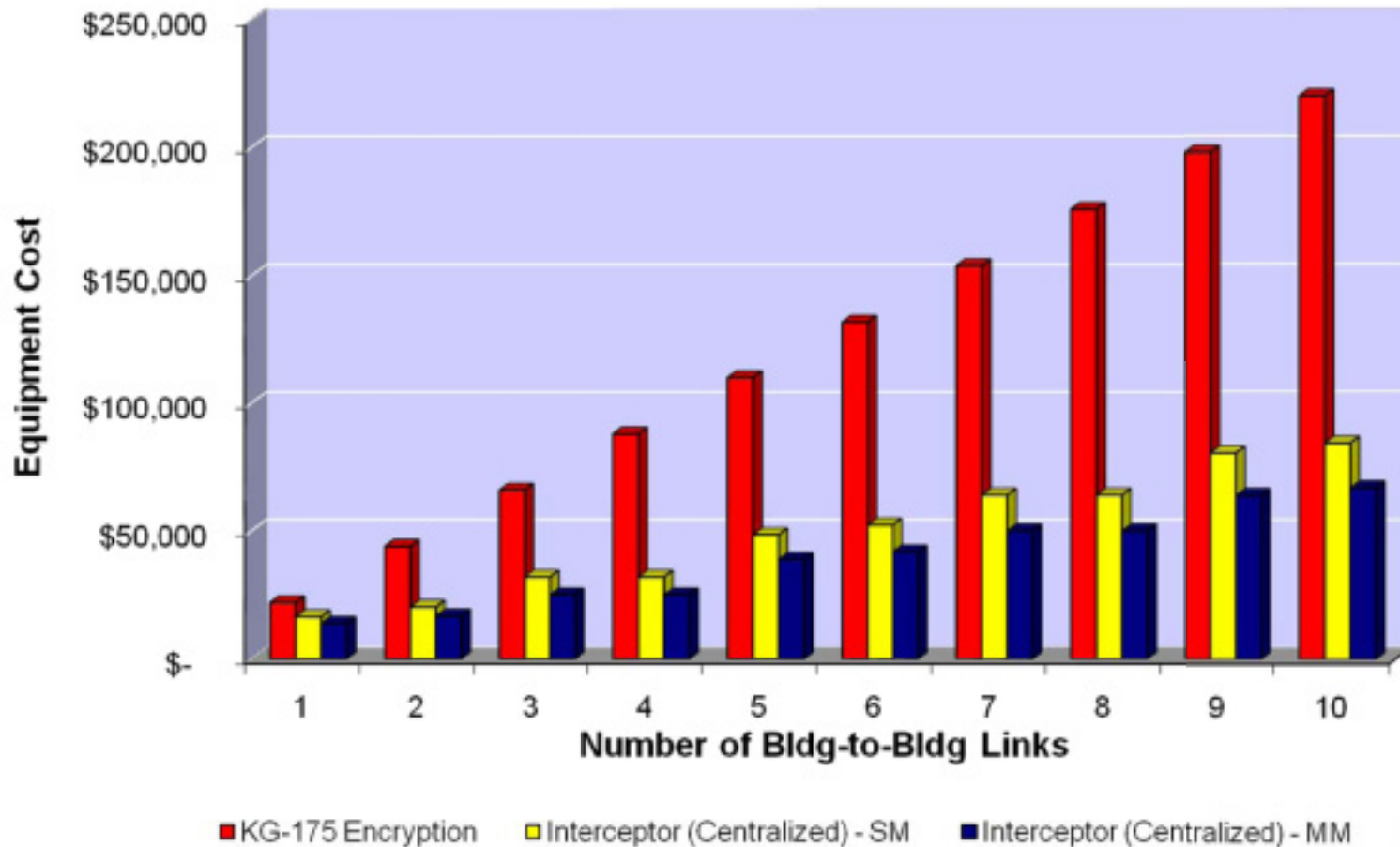
Bandwidth: **Unlimited**



Interceptor

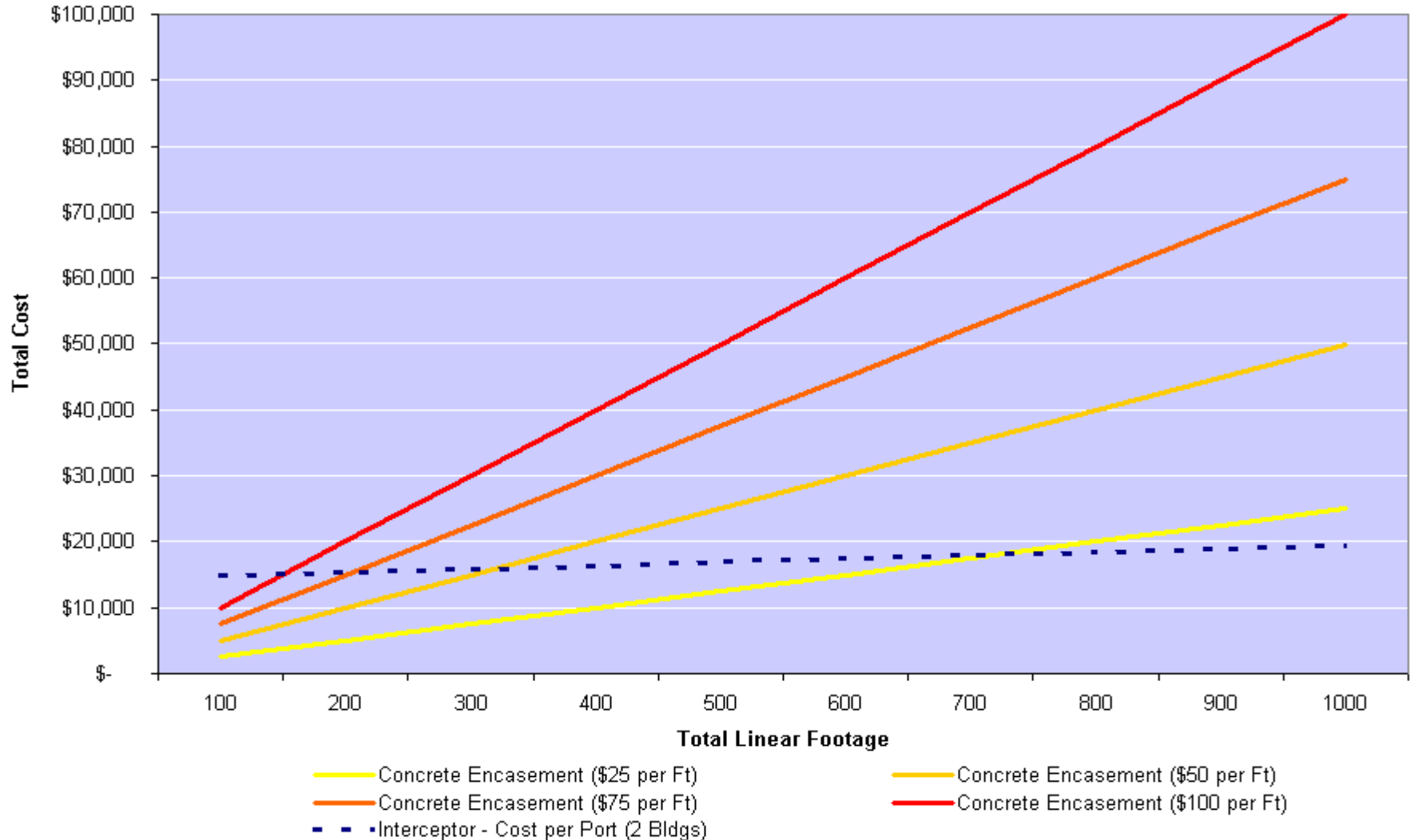
# Interceptor Cost Comparison: Building-to-Building vs. Encryption

Interceptor™ vs Encryption Equipment Costs



# Interceptor Cost Comparison: Building-to-Building vs. Concrete

Interceptor vs. Concrete Encasement  
*Two Building Links*



# Protecting Your Investment in Bandwidth

- Understanding the impact on the warfighter and the applications the depend upon is **ABSOLUTELY CRITICAL**
- Unlike commercial networks, C4ISR networks operate at **100% utilization** when crises arise...everyone will be on the net
- Scalability of encryption is a commonly overlooked criteria
  - How will the protection scale with 10 more users?
  - How about four more buildings?
  - What bottlenecks will this create?

**NetworkIntegrity**  
SYSTEMS

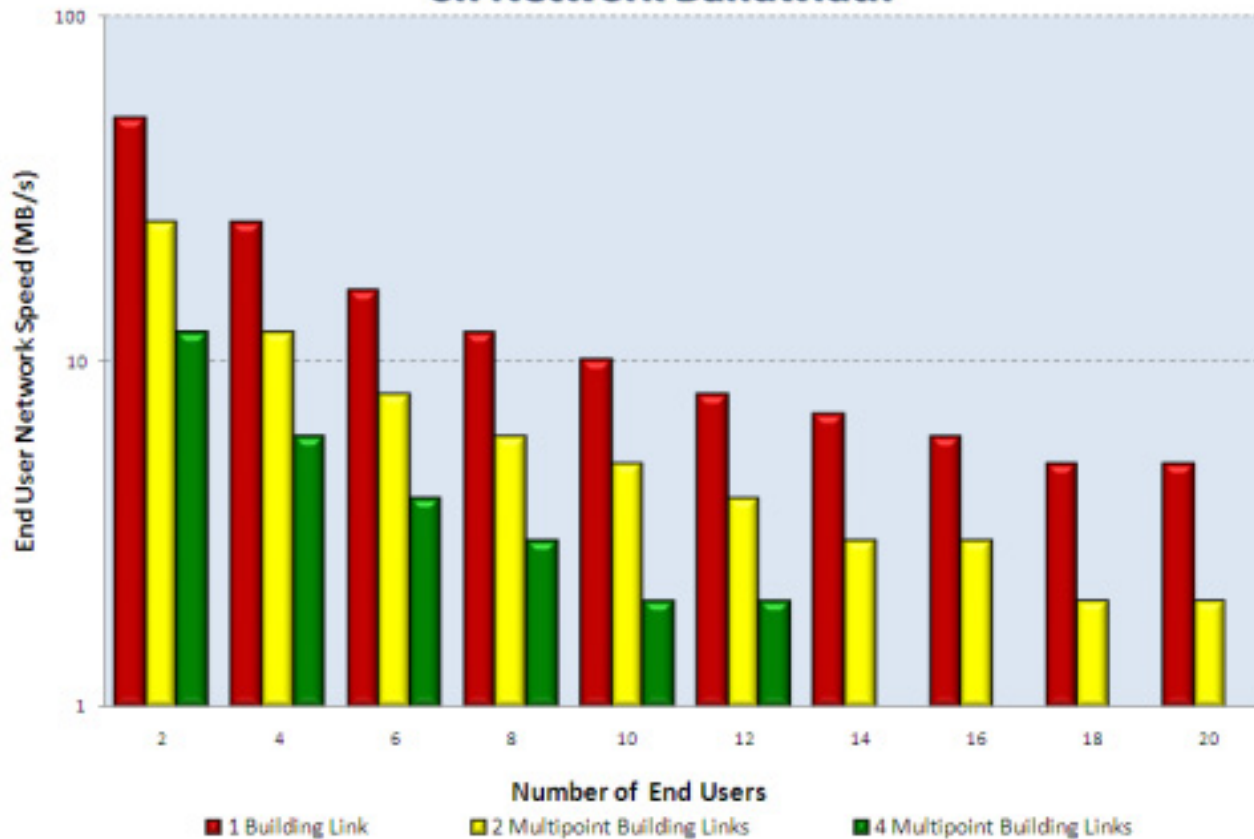
We Bring Security To Light™



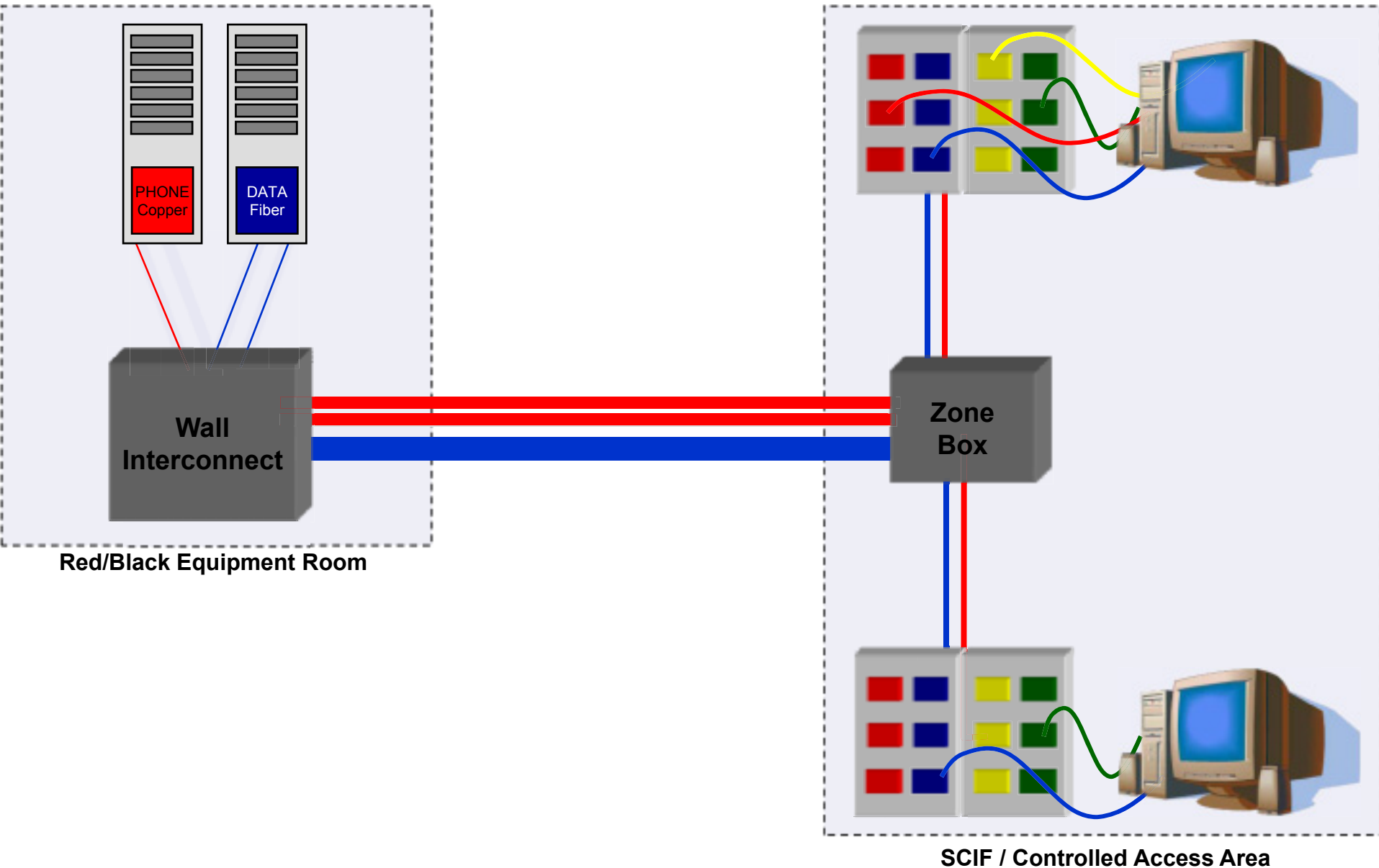
# Where's the Bottleneck?

## *Understanding Network Demand Modeling*

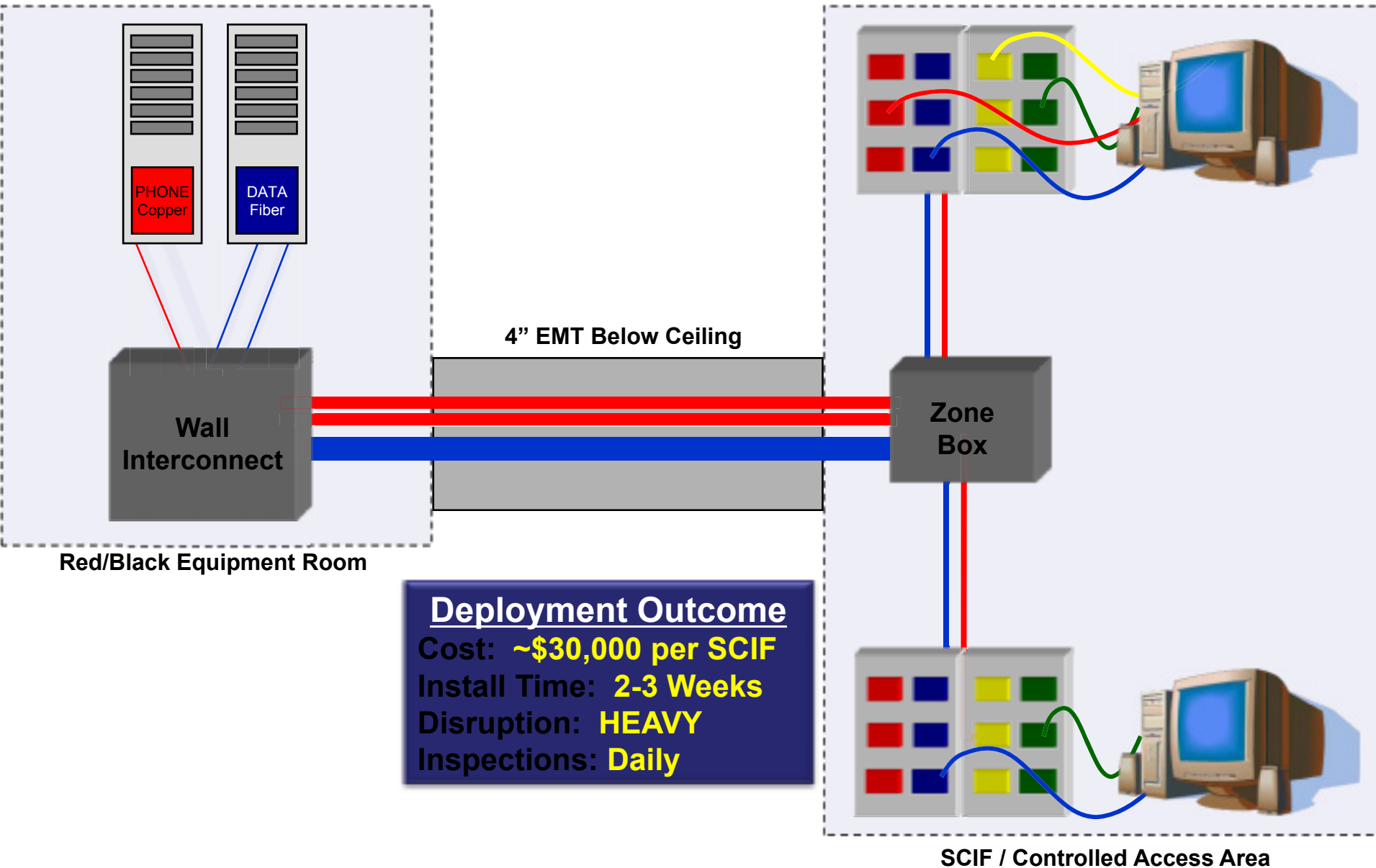
### Impact of Point-to-Multipoint Encryption on Network Bandwidth



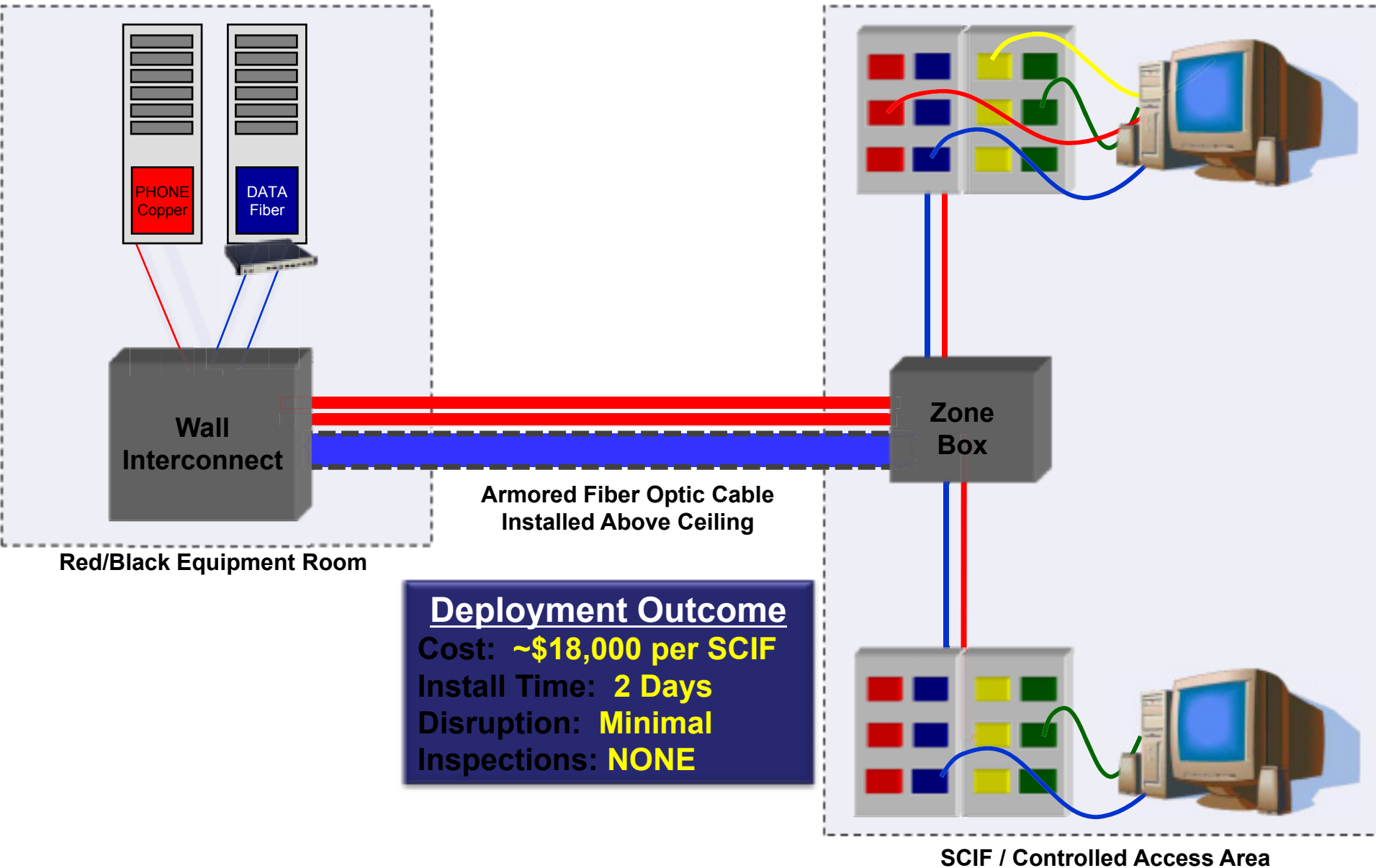
# Scenario: Provide SIPRNET Connection to a SCIF



# Hardened PDS



# Interceptor with Interlocking Armored Cable



# Summary Benefits:

## OSP Building-to-Building

- **32%** cost savings vs. encryption
- **80%** cost savings vs. concrete
- Can be ordered and installed in <50% of the time it would take for either of the other solutions
- Can be added to a single link on Day 1 and then seamlessly added to the other three links with no further work or reconfiguration

## Indoor SKIF

- **40%** cost savings for new deployments
- **20%** cost savings for legacy installations
- Improves building aesthetics - carrier can be hidden above the ceiling
- In some cases, carrier can be eliminated
- Eliminates the need for Periodic Visual Inspections (PVIs)
- Can be installed with minimal disruption to the facility
- Allows the upgrade of existing cables

# Interceptor Approvals

- **NRO + ISR** - Special Access Program & Contractor Facilities
  - *Locations undisclosed*
- **DIA** - JWICS (vis CTTA/EMSEC Office)
  - *Deployed at CENTCOM, S. Korea, VA*
- **USAF** - Alarmed Carrier Approved Products List
  - *AFI 33-201 - Communications Security: PDS Systems*
  - *Deployed at MacDill AFB, Scott AFB and Pentagon*
- **Navy** - (via SPAWAR CTTA and NETWARCOM)
  - *Basewide deployment at NUWC*
- **Army** - Reviewed through the G6 IA process and approved for use (alarm carrier)
  - *CRDA by INSCOM 2003*
- **DHS** - HS Information Network
  - *Interceptor is standard for DHS NCR*
- **DOJ** - FBI SCION Network + Terrorist Screening Center
  - *Deployed in Northern VA at multiple sites*



We Bring Security To Light™

LOCKHEED MARTIN

We never forget who we're working for®



NetworkIntegrity  
SYSTEMS

We Bring Security To Light™

National Aeronautics  
and Space Administration



**NORTHROP GRUMMAN**



MITRE

CSC



**GENERAL DYNAMICS**

# Interceptor Differentiators

## *INTERCEPTOR is...*



*...Flexible:* Users can move INTERCEPTORS around or add additional INTERCEPTORS as needed and at will

*...Scalable:* INTERCEPTOR protection can easily be added to additional or new network links and does not create any bandwidth limitations

*...Reliable:* INTERCEPTOR provides consistent protection and performance with no false alarms.

*...Affordable:* INTERCEPTOR typically saves between 30-80% of the cost of deployment over encryption and hardened carrier PDS. On certain deployments, armored cables can be used in place of EMT for further savings.

*...Proven:* INTERCEPTOR has been reviewed, tested, approved, and deployed by several other DoD services and C4ISR agencies with impeccable performance and protection