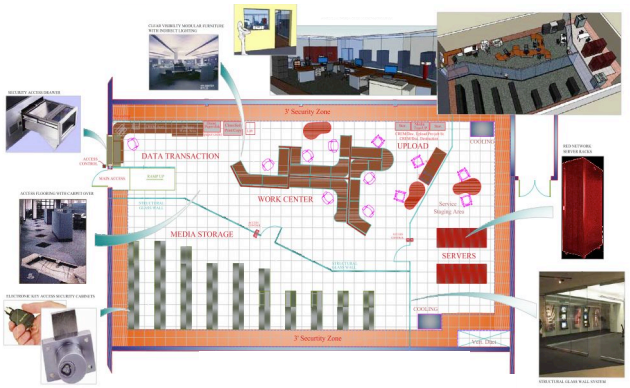
The Los Alamos Super Vault Type Room



May, 2008

Alex Kent

Advanced Computing Solutions
Program/Cyber Futures Laboratory

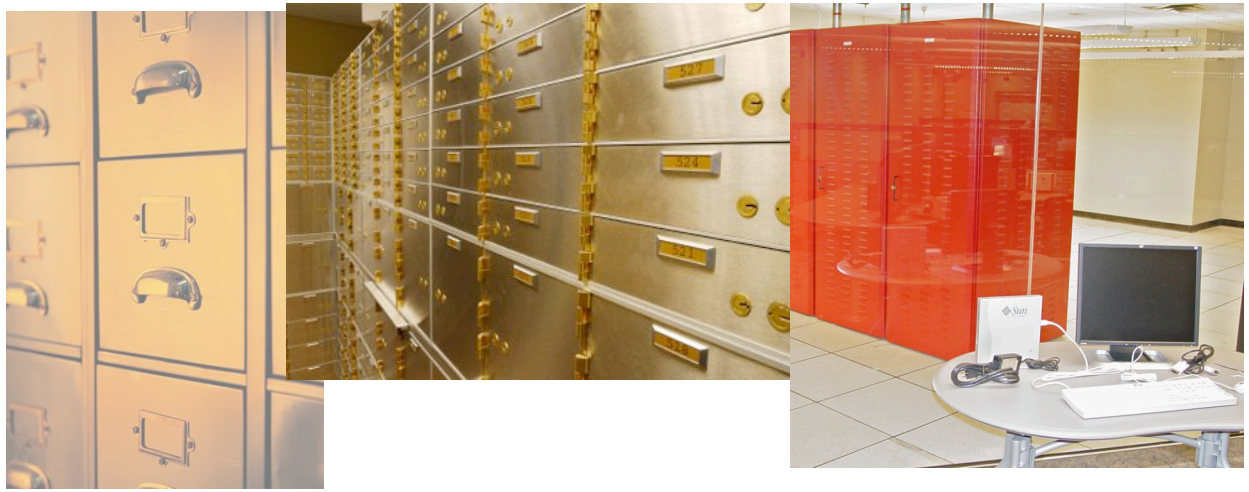
Los Alamos National Laboratory

Towards A Strategic Solution Space

- A decade of events…
  - Lost data/9-Points/Media incompatibility
  - Lost hard disks/Accountable Classified Removable Media
  - Lost barcodes/Increased ACREM accountability
  - Lost data/Thumb drives/Port blocking
- Commonality
  - Trusted insiders (cleared) doing inadvertent or purposeful actions resulting in loss
- Solution
  - More ubiquitous control and security of classified information both at rest and while in use
    - Yet still allow a productive work environment?

Think classified co-location facility managed like safety deposit boxes at a bank

- Compartmentalized, segregated control
- Professionally managed environment
- Full-service computer center
  - Cooling, power backup, etc
- System/data owners maintain final physical control



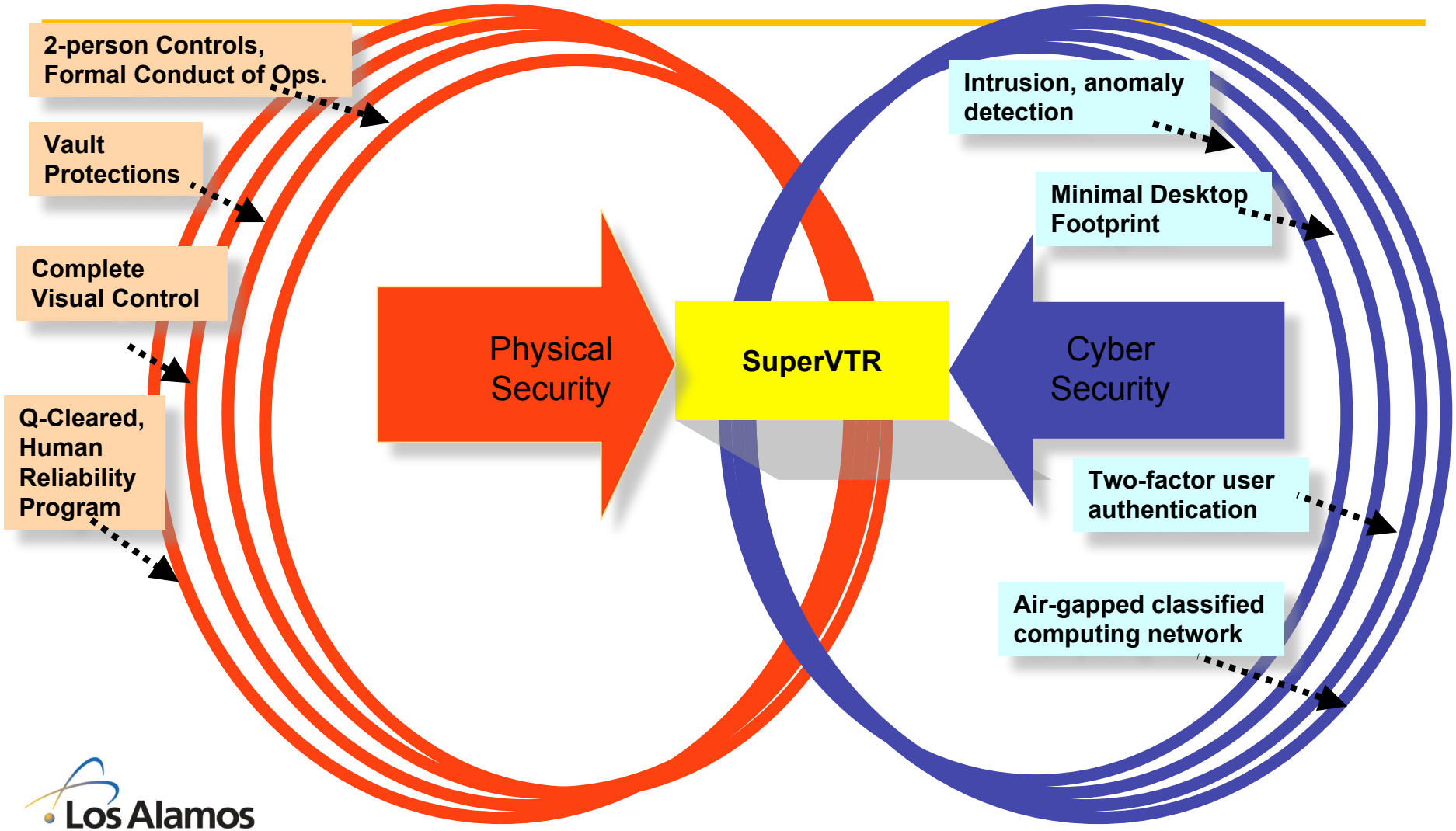
The Paradigm:
An Information/Data Glove Box

With data processing and storage residing within the well protected Super VTR environment:

- Users *can…*
  - Create, manipulate, and management classified information and data
- Users *cannot…*
  - Electronically extract or remove classified information and data

Residual vulnerability reduced to the single threat of capturing low-bandwidth screen/keyboard/mouse data only

Synergistic Integration of Physical and Cyber Security Layers



Integrated Safety and Security Management Human Performance Improvement

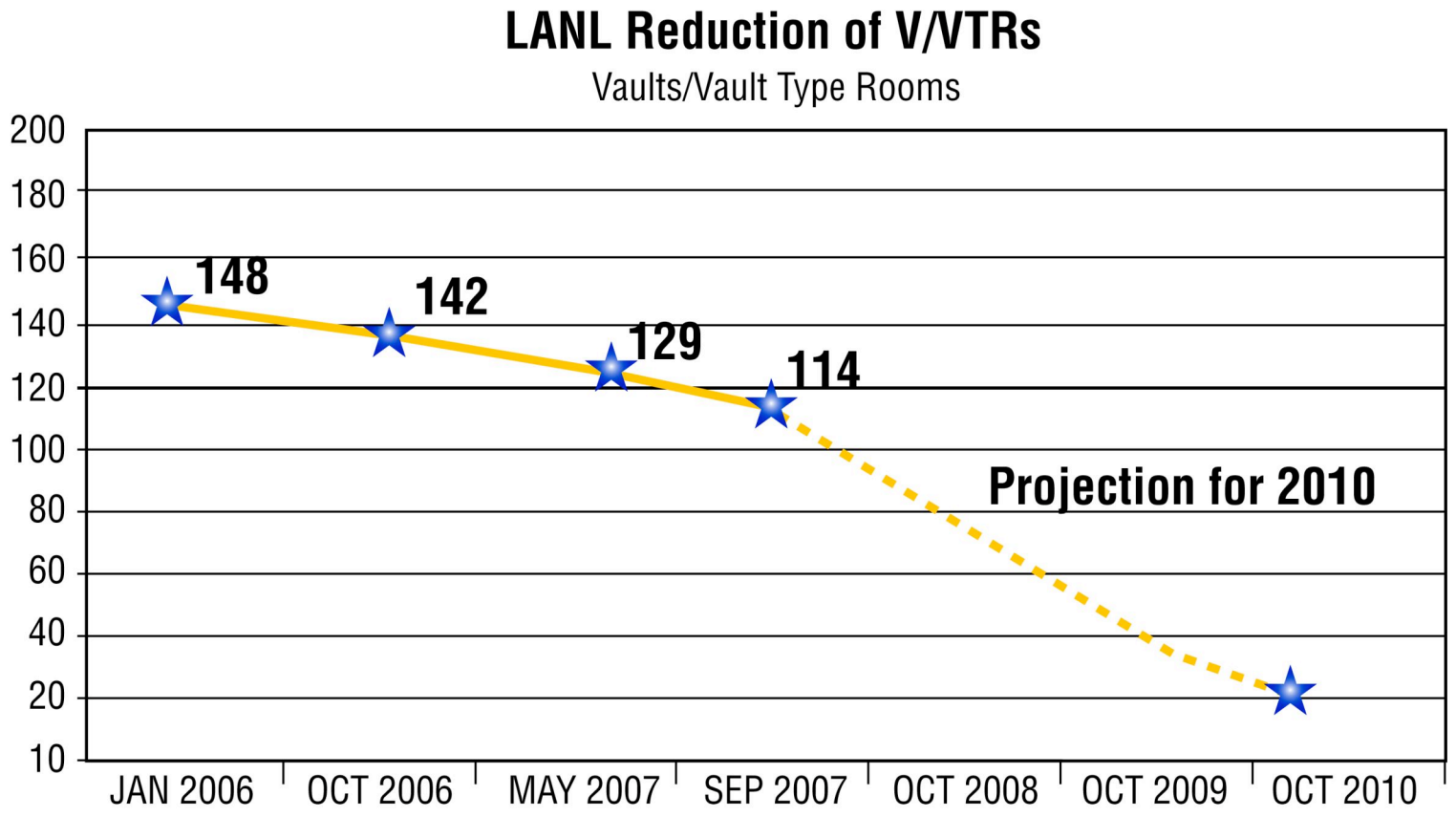
- Layered security
  - Separate and well defined user and processing environments
- Engineered controls
  - Centralized (server-side) control of user data ports
  - Constrained network environment
  - Simplified system management
- Reduced opportunity for error
  - Focus expertise and responsibility
  - KISS
- Increased user productivity

Cost Saving and Simplification

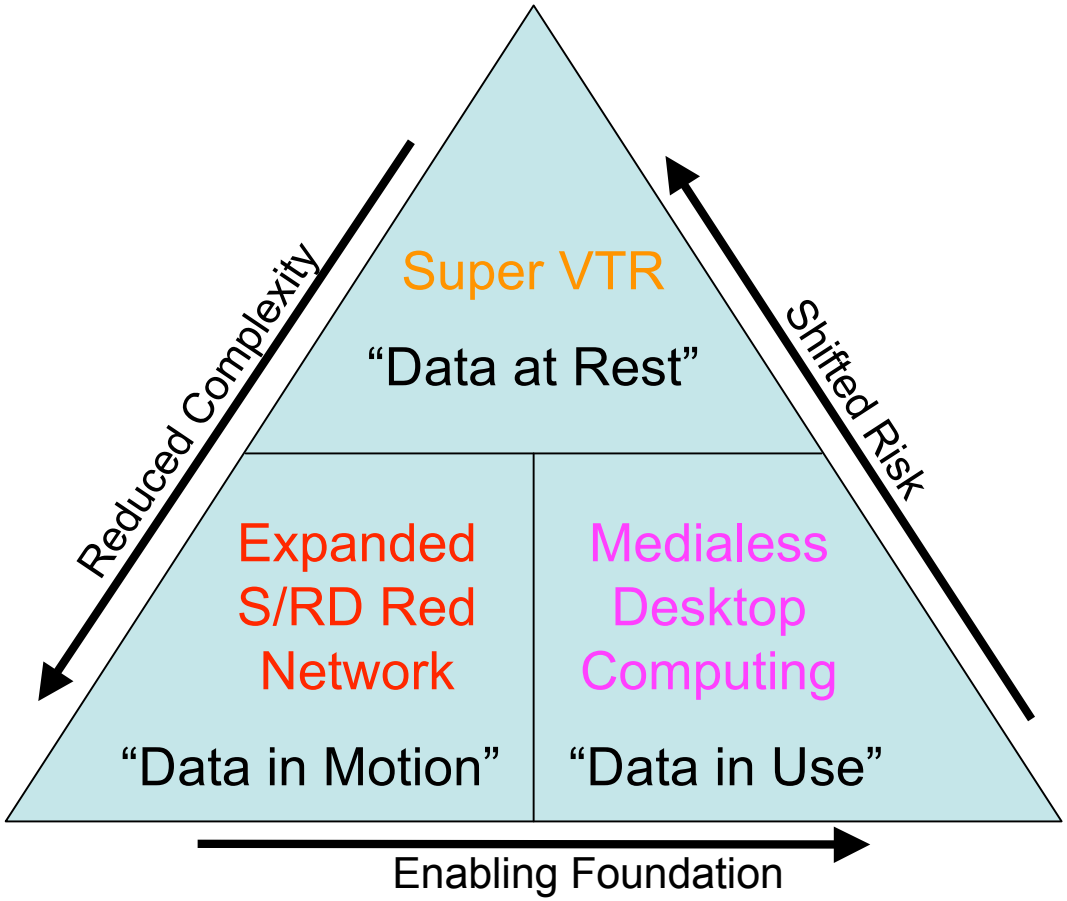
- Reduced information and physical security complexity
  - Reduced physical footprint
  - Reduced security services
  - Reduced risk of costly security incidents
- Close down existing vaults and related staffing
- Avoid vault sensor and alarm upgrade costs
- Reduced security costs for desktops and related protections
- Reduced VTR/Cyber security related work required by programmatic staff

… while substantially *increasing* security and programmatic productivity

Reduced Physical Vulnerability



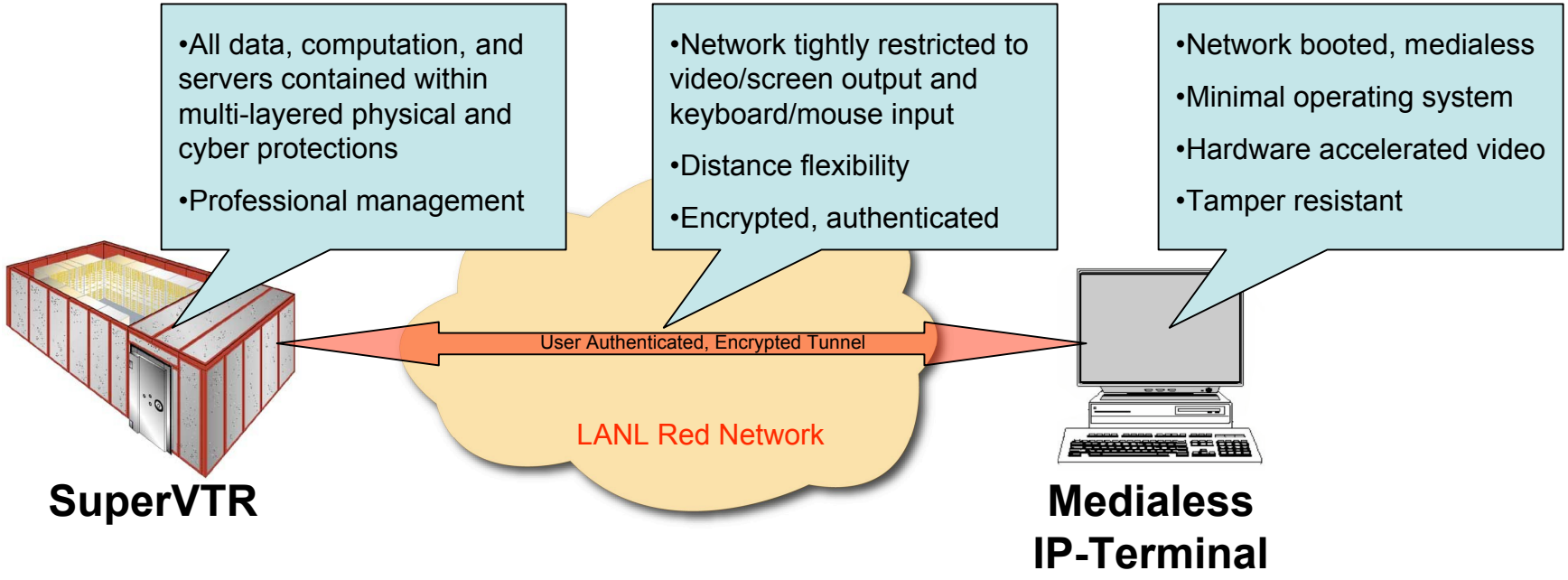
Comprehensive Classified Computing Capability



Moving the vulnerability/threat space from the office environment to the Super VTR

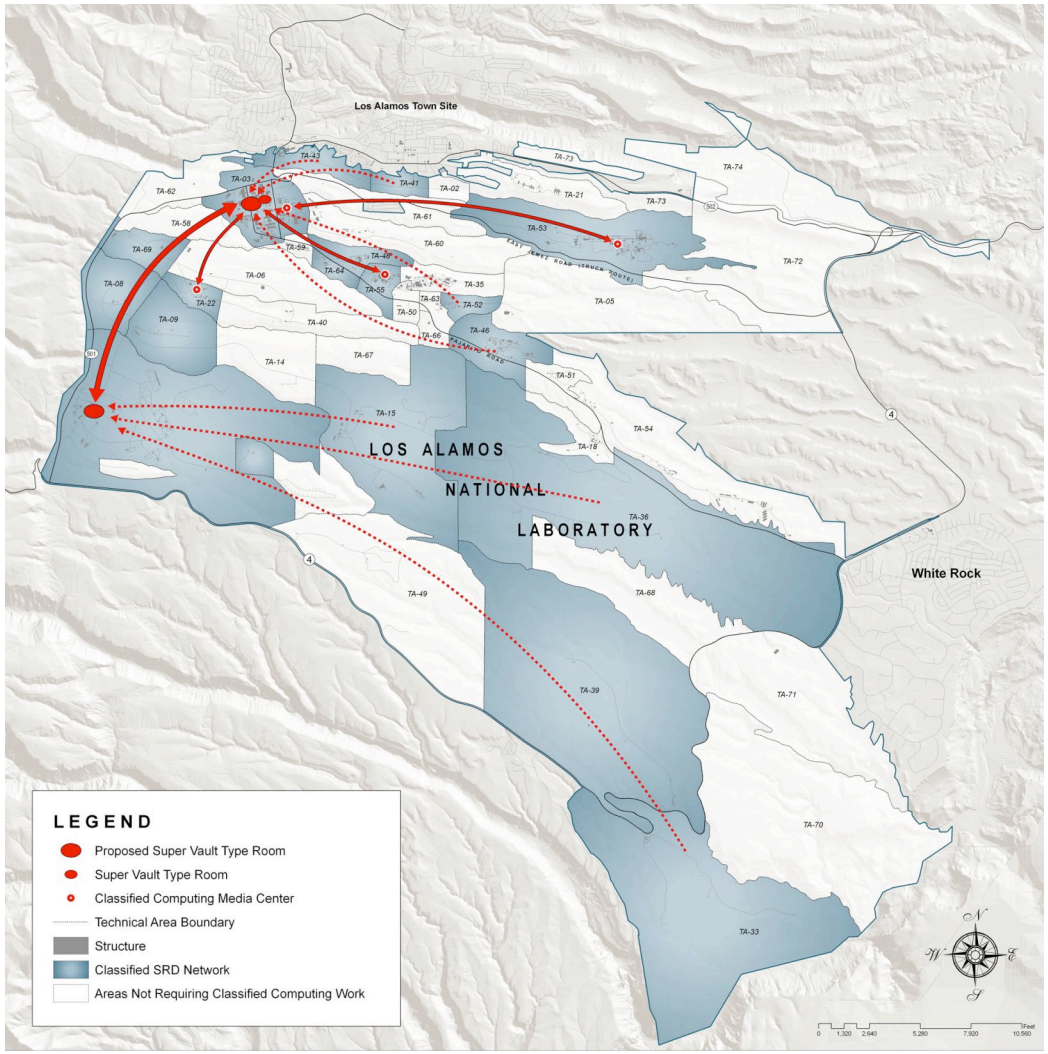
- Medialess office computing, minimal electronics
- Finite selection of strongly vetted medialess desktop options
- All data storage and control exists only within the Super VTR
- Systems approach with complete end-to-end security
- Specialized, restricted IP network outside of SVTR that only allows medialess computing protocols to transit
- Increased anomaly detection designed specific to the risks, threats, and vulnerabilities of a classified, air-gapped network
- Agility to respond to future threats and requirements

Ubiquitous end-to-end security with robust usability



See Ahmad Douglas' NLIT08 talk on Medialess Computing for a comprehensive overview

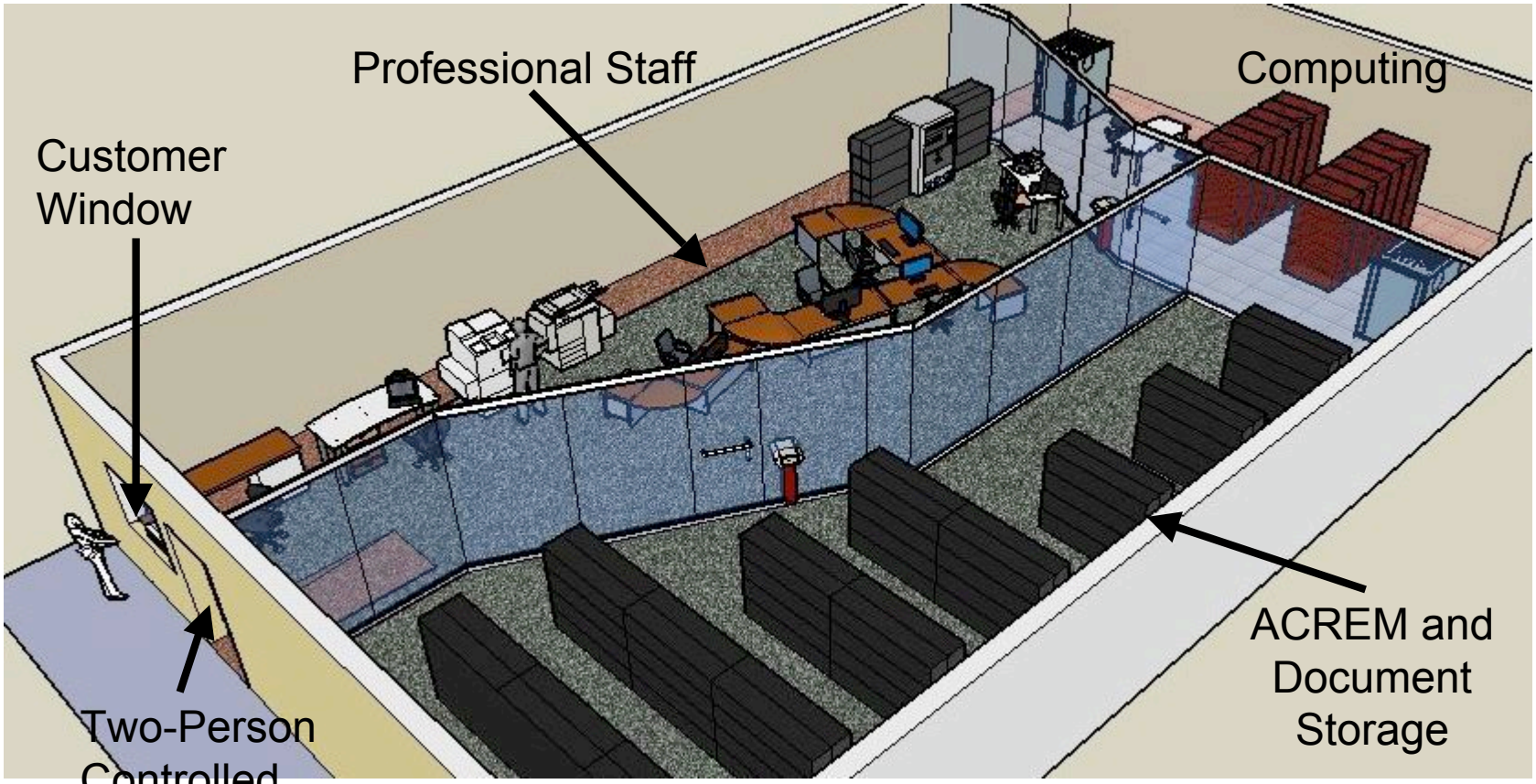
The Network: Tying it together



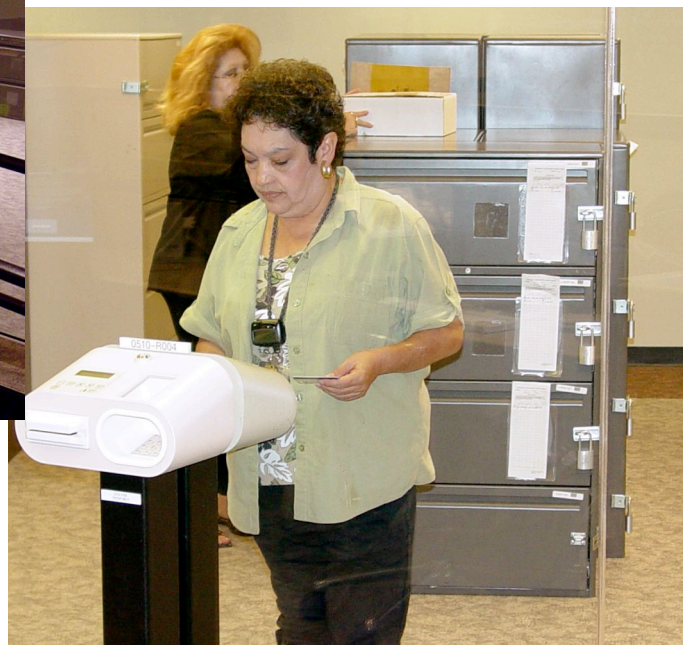
The Super VTR Prototype

- Planning began in Spring 2007, went operational in Summer 2007
  - Remodeled room within an existing computing facility
- Focused on demonstrated both the physical and cyber concepts and integration
- Understanding that it was insufficient to meet the entire Laboratory's needs
- Currently in full operation
  - Contains and services approximately 75% of LANL's classified ACREM
  - Provides classified medialess computing service to approximately ~150 users
  - Currently under expansion for supporting SIPRnet and other classified computing with estimates to serve an additional 200 users
  - Other information services available

Super VTR Prototype Cutout View

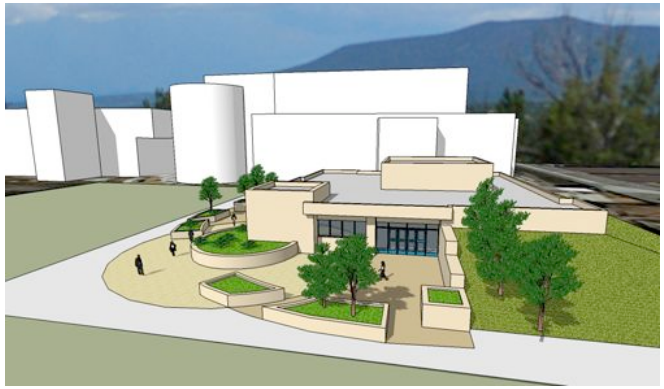


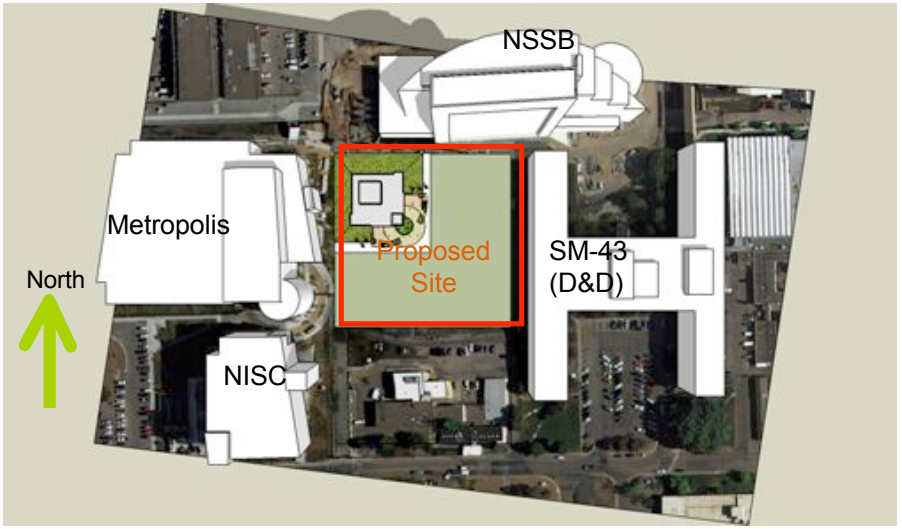
Operational Super VTR Prototype



From Prototype to Full Scale

- Funding provided in LANL FY08 budget
- Planning underway
- Central standalone facility within main (TA-3) site
- Backup facility to follow





Enabled Future Technologies

- Physical Security
  - Video monitoring and surveillance of the SVTR
  - Programmatic key control
  - RF control
  - RFID tagging
  - Biometrics
- Cyber Security
  - Printed document water marks
  - Fully realized PL-3 cyber environment
  - STE bridge and audio capability on desktops (VoIP)
  - Authenticated print/copy/scan system
  - Security anomaly detection on cyber+physical

Questions?

Contact Information:

Alex Kent (alex@lanl.gov)

Scott Miller (samiller@lanl.gov)