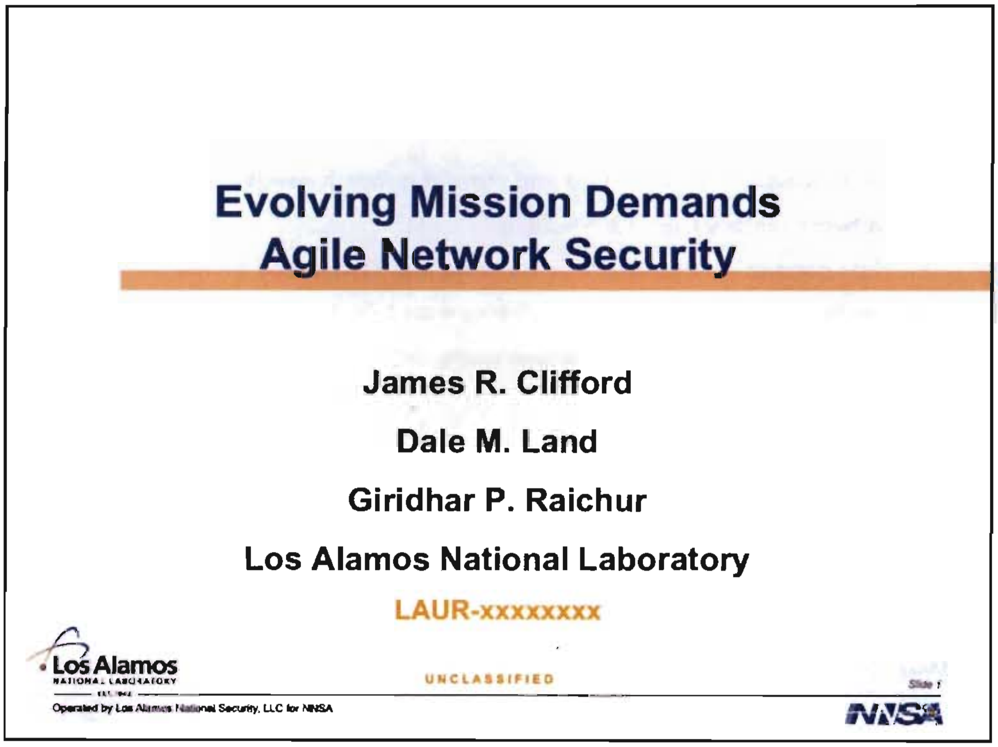
Title: Evolving Mission Demands Agile Network Security

Author(s): James R. Clifford
Dale M. Land
Giridhar P. Raichur

Intended for: NSA Trusted Computing Conference and Exposition
Orlando, FL
September 20- 22, 2011



Evolving Mission Demands Agile Network Security

James R. Clifford

Dale M. Land

Giridhar P. Raichur

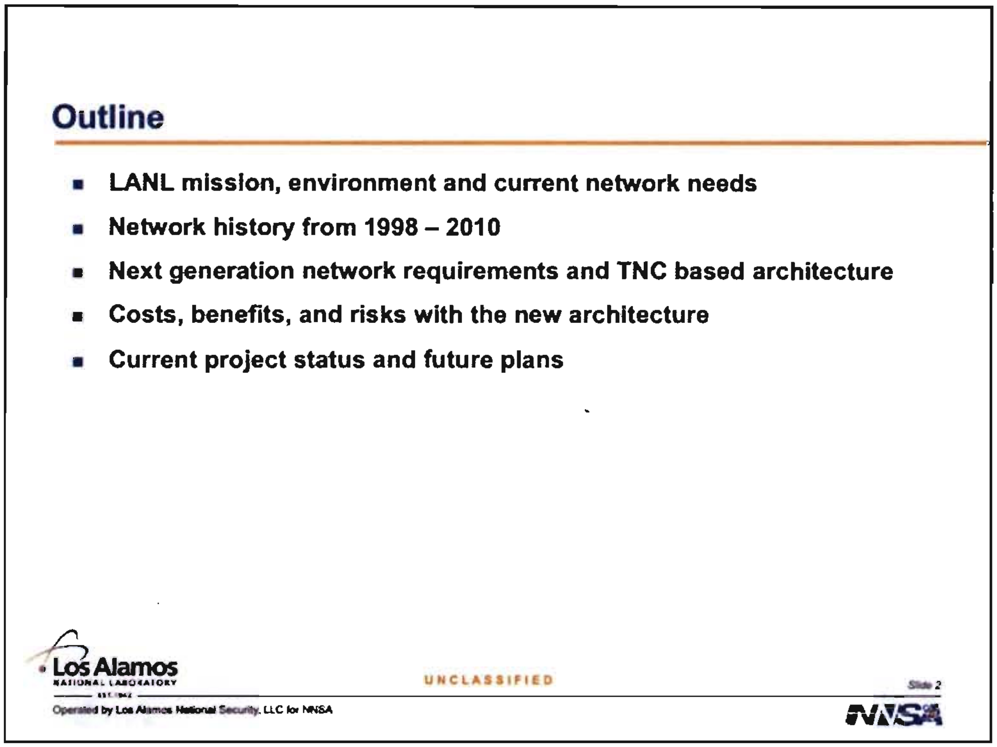
Los Alamos National Laboratory

LAUR-xxxxxxxx

UNCLASSIFIED

Slide 1

Operated by Los Alamos National Security, LLC for NNSA



Outline

- LANL mission, environment and current network needs
- Network history from 1998 – 2010
- Next generation network requirements and TNC based architecture
- Costs, benefits, and risks with the new architecture
- Current project status and future plans

Los Alamos NATIONAL LABORATORY EST. 1943

UNCLASSIFIED

Slide 2

Operated by Los Alamos National Security, LLC for NNSA

NNSA

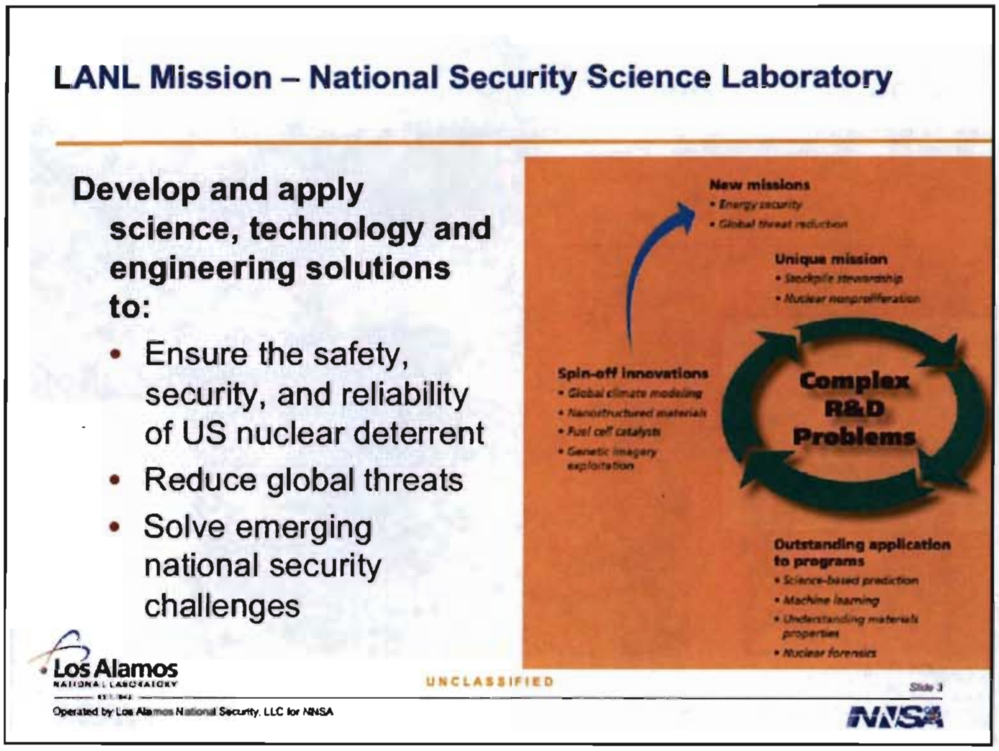
First describe the LANL environment for context (5 minutes)

Show we have been adapting from no firewall to 2010 (5 minutes)

Show the TNC standards based architecture and how it works to meet new requirements (15 minutes)

Current and future benefits, costs, and risks.

Current status and next steps (5 minutes)



LANL Mission – National Security Science Laboratory

Develop and apply science, technology and engineering solutions to:

- Ensure the safety, security, and reliability of US nuclear deterrent
- Reduce global threats
- Solve emerging national security challenges

New missions
- *Energy security*
- *Global threat reduction*

Unique mission
- *Stockpile stewardship*
- *Nuclear nonproliferation*

Spin-off innovations
- *Global climate modeling*
- *Nanostructured materials*
- *Fuel cell catalysts*
- *Genetic imagery exploitation*

Complex R&D Problems

Outstanding application to programs
- *Science-based prediction*
- *Machine learning*
- *Understanding materials properties*
- *Nuclear forensics*

Los Alamos NATIONAL LABORATORY

UNCLASSIFIED

Slide 3

Operated by Los Alamos National Security, LLC for NNSA

NNSA

7th decade of nuclear weapons stewardship

Global security challenges - WMD, terrorism, energy demand, natural events on regions and societies - call for innovative scientific and technological responses.\

Partner with laboratories, universities, and industries (CRADAs)

Underlying Strategy

Invest in and leverage science that matters

Agility in creating teams with partners

Transform our scientific campus

Program Diversity

Los Alamos
NATIONAL LABORATORY
EST. 1943

UNCLASSIFIED

Slide 4

Operated by Los Alamos National Security, LLC for NNSA

NNSA

Roadrunner

First tera scale high performance computer

Unclassified clusters and storage for collaboration

Predictive science through HPC modelling;

Global ocean climate model

Nuclear weapon stockpile stewardship

LANSCE

Neutron Scattering

User facility with visiting scientists from around the world

AngelFire

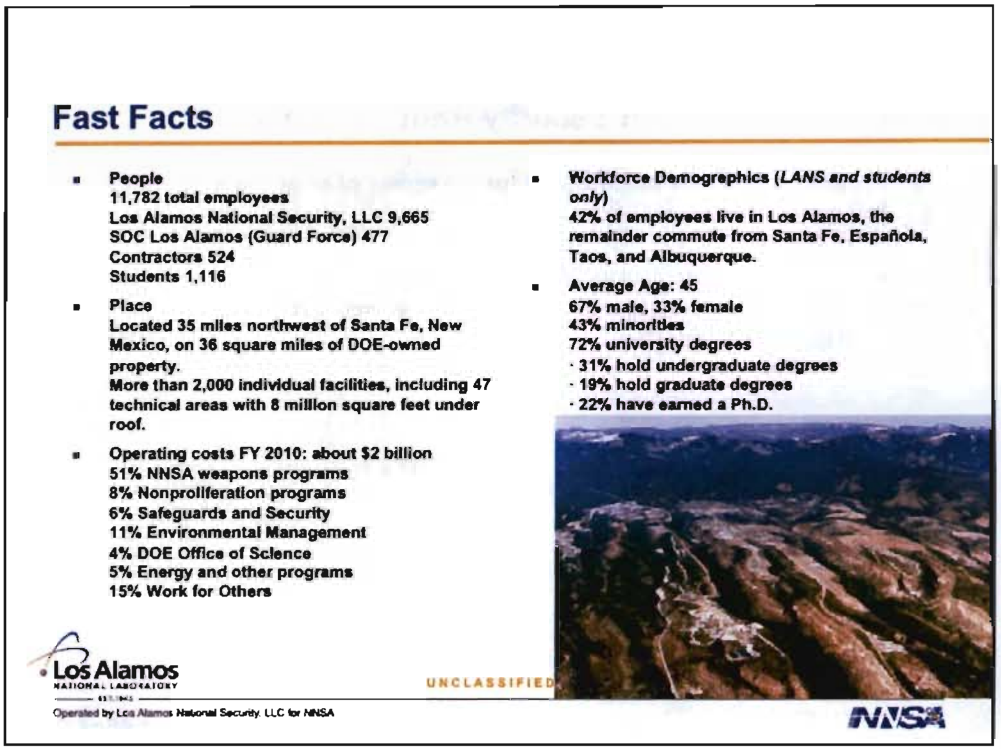
Advance digital image processing and decision support save lives in IRAQ

Real time, high resolution surveillance over a wide area, zoom and replay

Tested and fielded 18 months with Air Force Research Lab and USMC

NSSB and main campus

The usual IT: Building Automation, Communications mail, phones, video, HR, Financials



Fast Facts

- People
  11,782 total employees
  Los Alamos National Security, LLC 9,665
  SOC Los Alamos (Guard Force) 477
  Contractors 524
  Students 1,116
- Place
  Located 35 miles northwest of Santa Fe, New Mexico, on 36 square miles of DOE-owned property.
  More than 2,000 individual facilities, including 47 technical areas with 8 million square feet under roof.
- Operating costs FY 2010: about $2 billion
  51% NNSA weapons programs
  8% Nonproliferation programs
  6% Safeguards and Security
  11% Environmental Management
  4% DOE Office of Science
  5% Energy and other programs
  15% Work for Others
- Workforce Demographics (*LANS and students only*)
  42% of employees live in Los Alamos, the remainder commute from Santa Fe, Española, Taos, and Albuquerque.
- Average Age: 45
  67% male, 33% female
  43% minorities
  72% university degrees
  · 31% hold undergraduate degrees
  · 19% hold graduate degrees
  · 22% have earned a Ph.D.

UNCLASSIFIED

Operated by Los Alamos National Security, LLC for NNSA

IT Customers

Employees - scientists, engineers, technicians, administration, business support, crafts staff

Students and interns

Contractors - on-site and off-site

Visitors

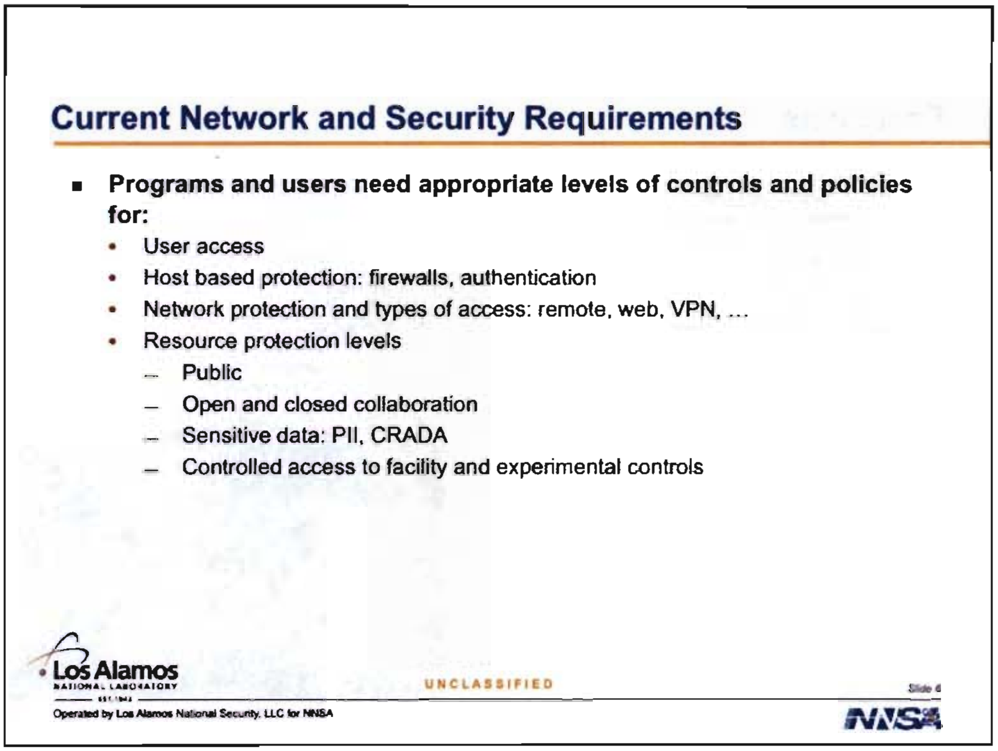
Collaborators

Employees on assigment in Washington, DC and Albuquerque

Roughly 10,000 employess and 4,000 external

36 sq. mile campus , over 1/2 the size of Washington, DC.

Plus leased space in town, remote offices in Carlsbad, Nevada and more.



Current Network and Security Requirements

- **Programs and users need appropriate levels of controls and policies for:**
  - User access
  - Host based protection: firewalls, authentication
  - Network protection and types of access: remote, web, VPN, …
  - Resource protection levels
    - Public
    - Open and closed collaboration
    - Sensitive data: PII, CRADA
    - Controlled access to facility and experimental controls

Los Alamos NATIONAL LABORATORY EST. 1943

UNCLASSIFIED

Slide 6

Operated by Los Alamos National Security, LLC for NNSA

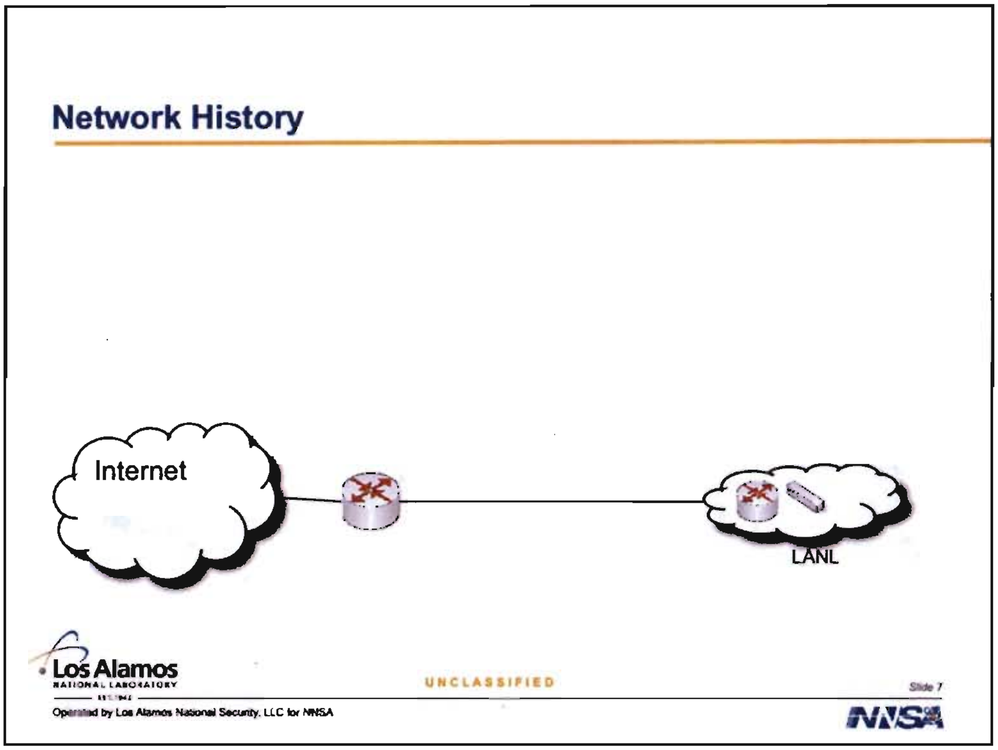
NNSA

User access includes more than just employee or just two levels: all and none

Host protections, policy or health check or registrations differ based on business need.

Network ingress and egress policies and methods differ

Mixed data in the same boundary results in network protections that are too severe for some but too lenient for others.



Network History

Los Alamos
NATIONAL LABORATORY
EST. 1943

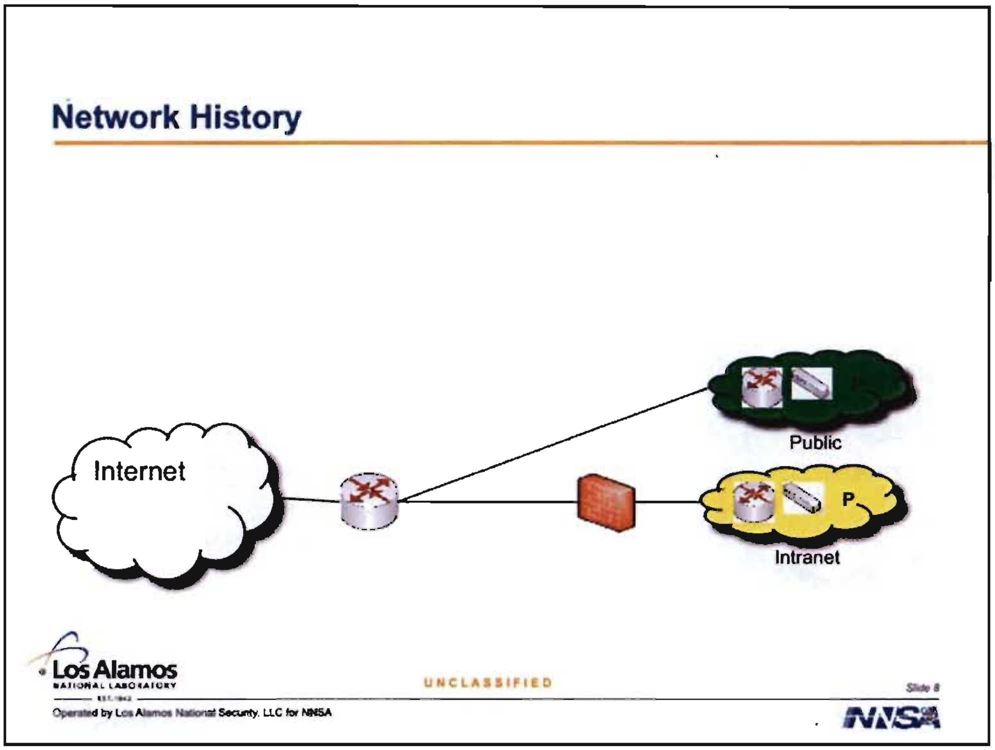
UNCLASSIFIED

Slide 7

Operated by Los Alamos National Security, LLC for NNSA

NNSA

Before 1998 there was no firewall



Network History

Internet

Public

P

Intranet

UNCLASSIFIED

Slide 8

Los Alamos NATIONAL LABORATORY EST. 1943

Operated by Los Alamos National Security, LLC for NNSA

NNSA

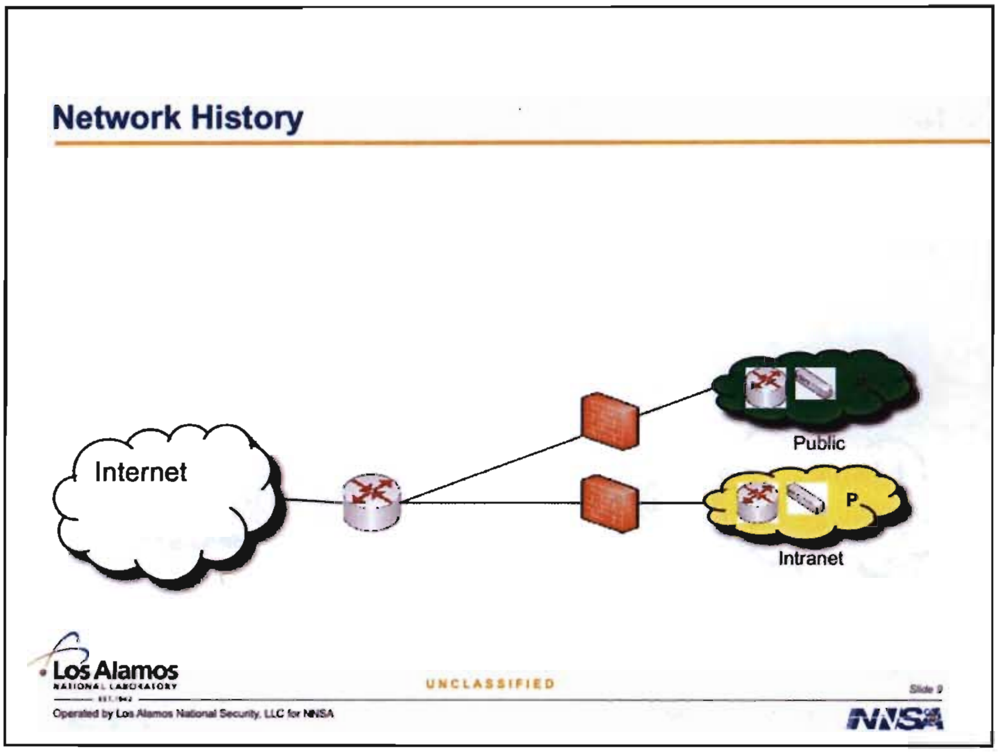
The first, and future firewalls, was Linux with IPtables.

More of a marketing effort and cultural change than technical.

Public facing systems had no protection.

Lots of users wanted to live in the DMZ.

Policy board decided what was DMZ worthy.



Network History

Los Alamos
NATIONAL LABORATORY
EST. 1943

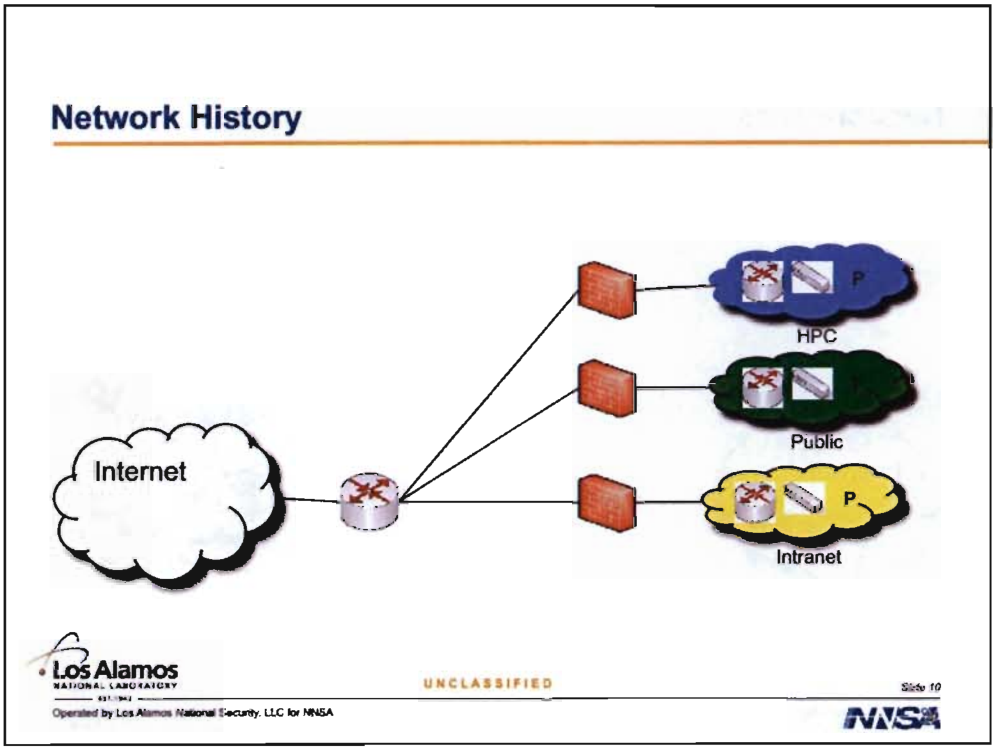
UNCLASSIFIED

Slide 9

Operated by Los Alamos National Security, LLC for NNSA

NNSA

Second firewall gave DMZ defense in depth network protection.



Network History

Los Alamos
NATIONAL LABORATORY
EST. 1943

UNCLASSIFIED

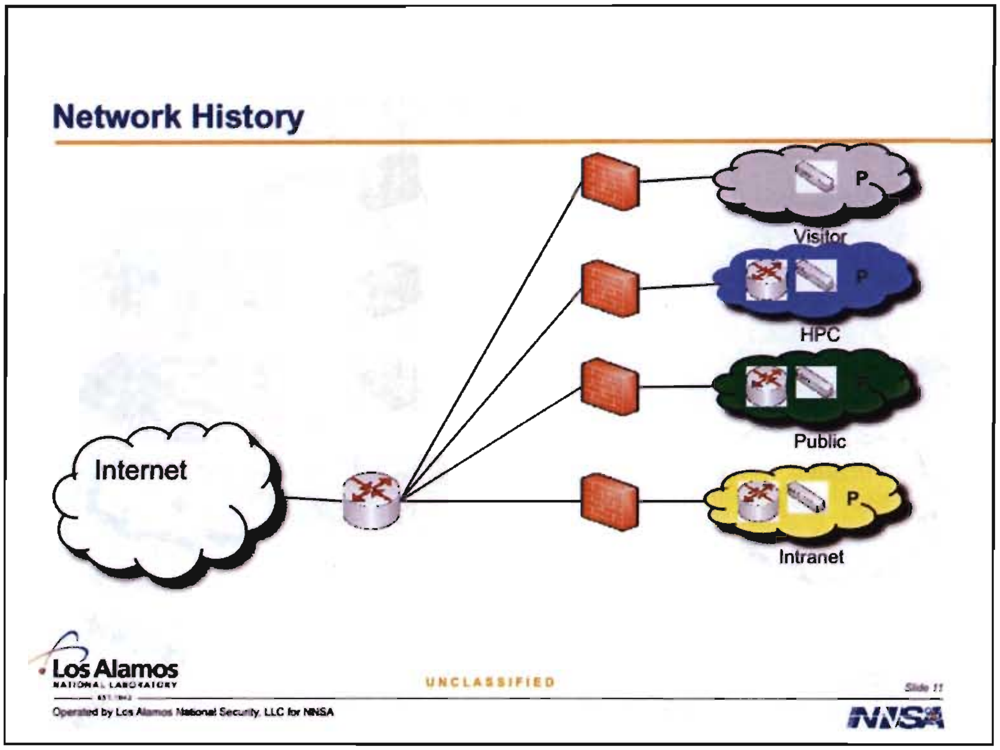
Slide 10

Operated by Los Alamos National Security, LLC for NNSA

NNSA

HPC moved some resources to new enclave in response to widespread security incident

A new board for managing policy and change.



Network History

Los Alamos
NATIONAL LABORATORY
EST. 1943

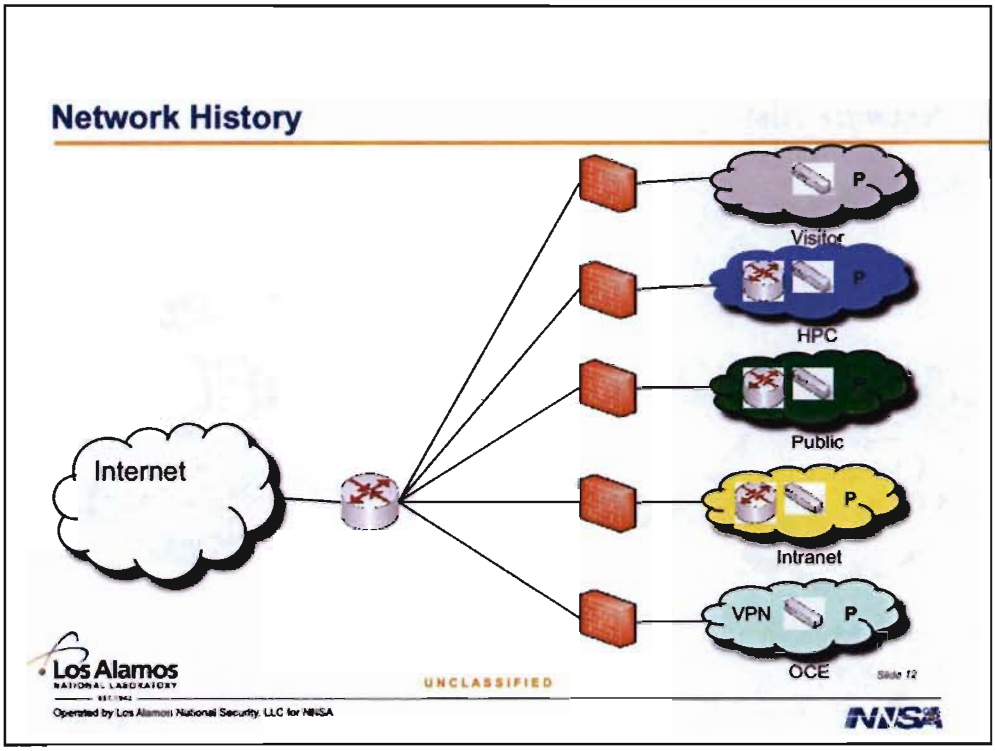
UNCLASSIFIED

Slide 11

Operated by Los Alamos National Security, LLC for NNSA

NNSA

Visitors were arriving with laptops. We did not want visitors or their computers on the intranet; bad for security and hard on the visitors. More policy.



Network History

Los Alamos NATIONAL LABORATORY EST. 1943

UNCLASSIFIED

Slide 12

Operated by Los Alamos National Security, LLC for NNSA

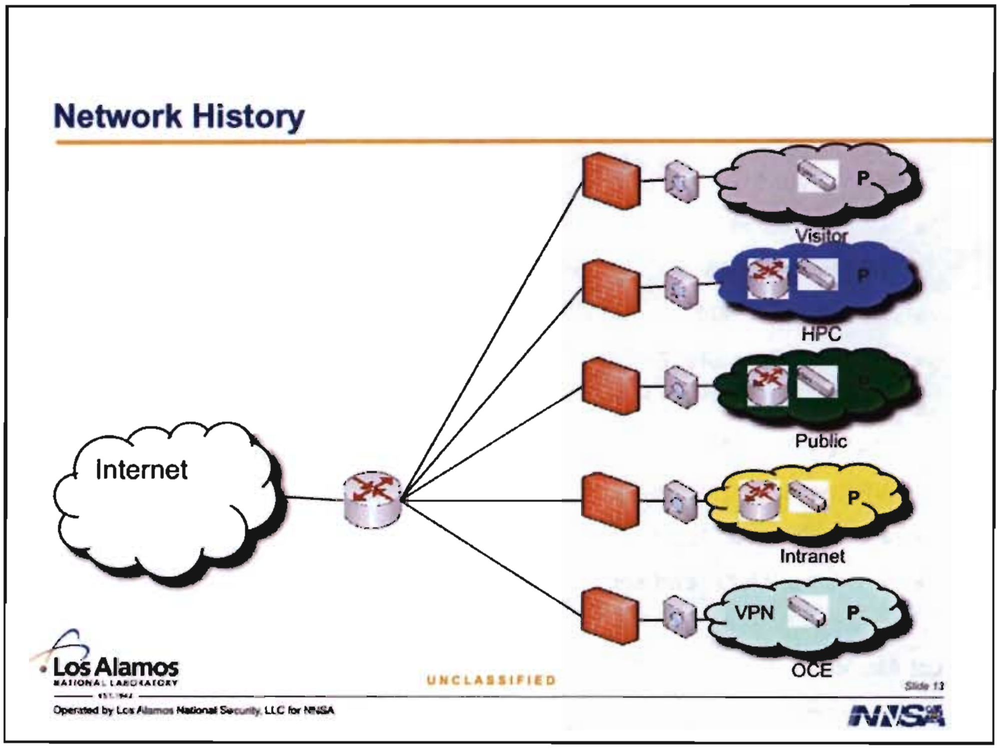
NNSA

Created primarily for Foreign national working on open science so they would not have to use the intranet.

VPN overlay on top of the intranet with high maintenance; the most practical to implement of several solutions.

Role based firewall and access controls to get to intranet services.

Still need to rethink where how services are provisioned. Scattered servers with differing access methods is hard to administer.



Network History

Los Alamos
NATIONAL LABORATORY
EST. 1943

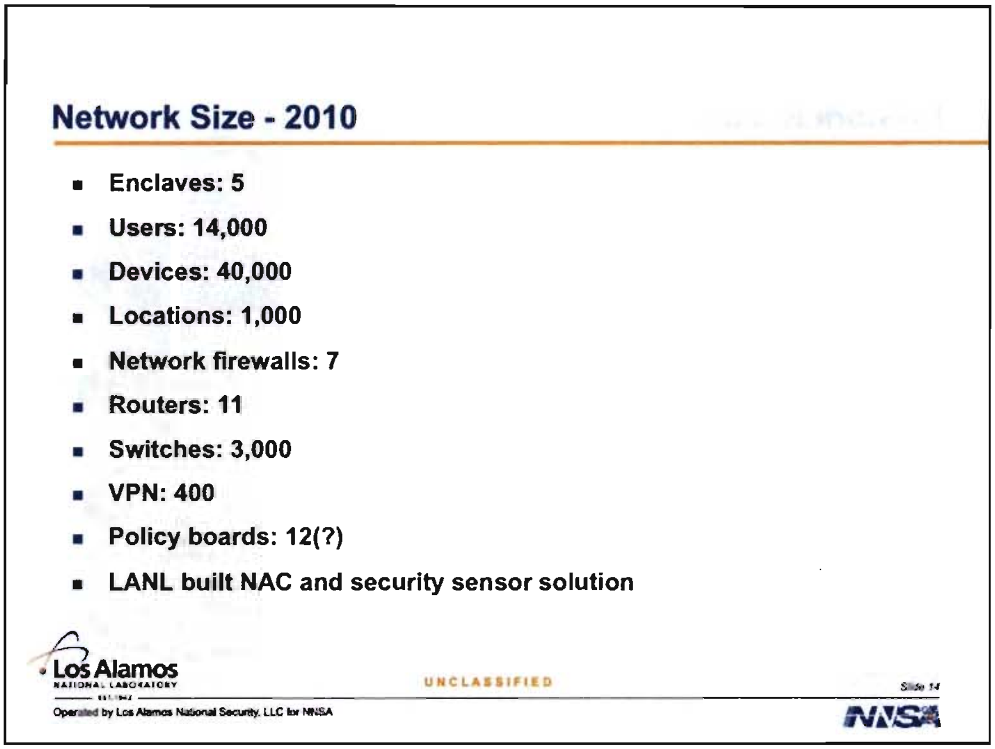
UNCLASSIFIED

Slide 13

Operated by Los Alamos National Security, LLC for NNSA

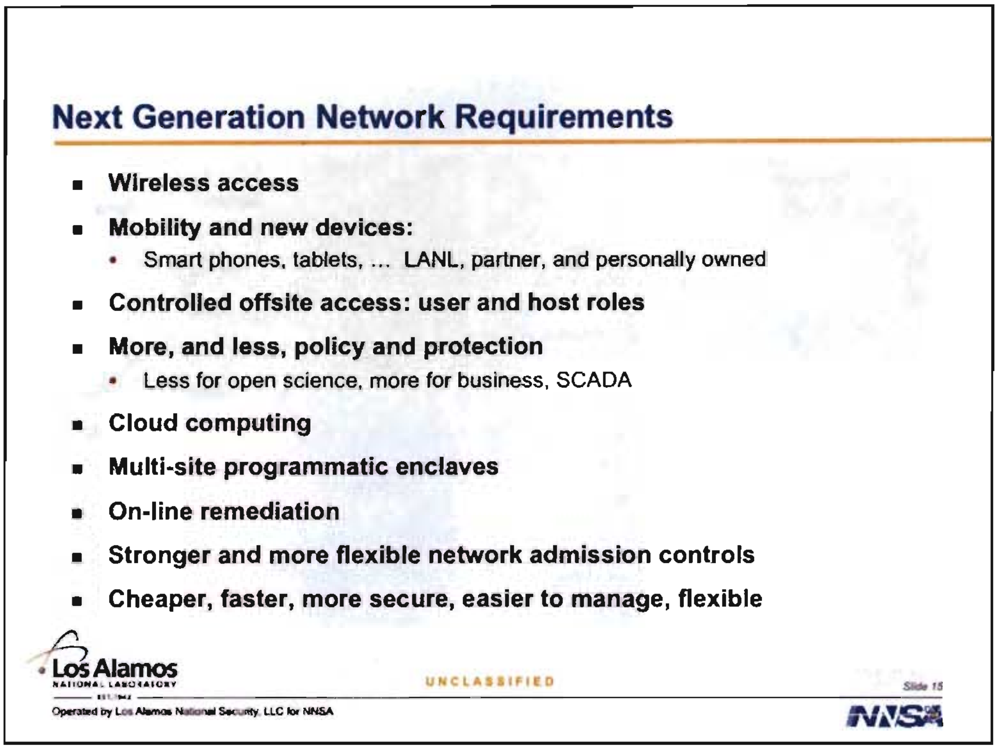
NNSA

Added IDS and IPS for each enclave.



Network Size - 2010

- Enclaves: 5
- Users: 14,000
- Devices: 40,000
- Locations: 1,000
- Network firewalls: 7
- Routers: 11
- Switches: 3,000
- VPN: 400
- Policy boards: 12(?)
- LANL built NAC and security sensor solution



Next Generation Network Requirements

- Wireless access
- Mobility and new devices:
  - Smart phones, tablets, … LANL, partner, and personally owned
- Controlled offsite access: user and host roles
- More, and less, policy and protection
  - Less for open science, more for business, SCADA
- Cloud computing
- Multi-site programmatic enclaves
- On-line remediation
- Stronger and more flexible network admission controls
- Cheaper, faster, more secure, easier to manage, flexible

Los Alamos NATIONAL LABORATORY EST. 1943

UNCLASSIFIED

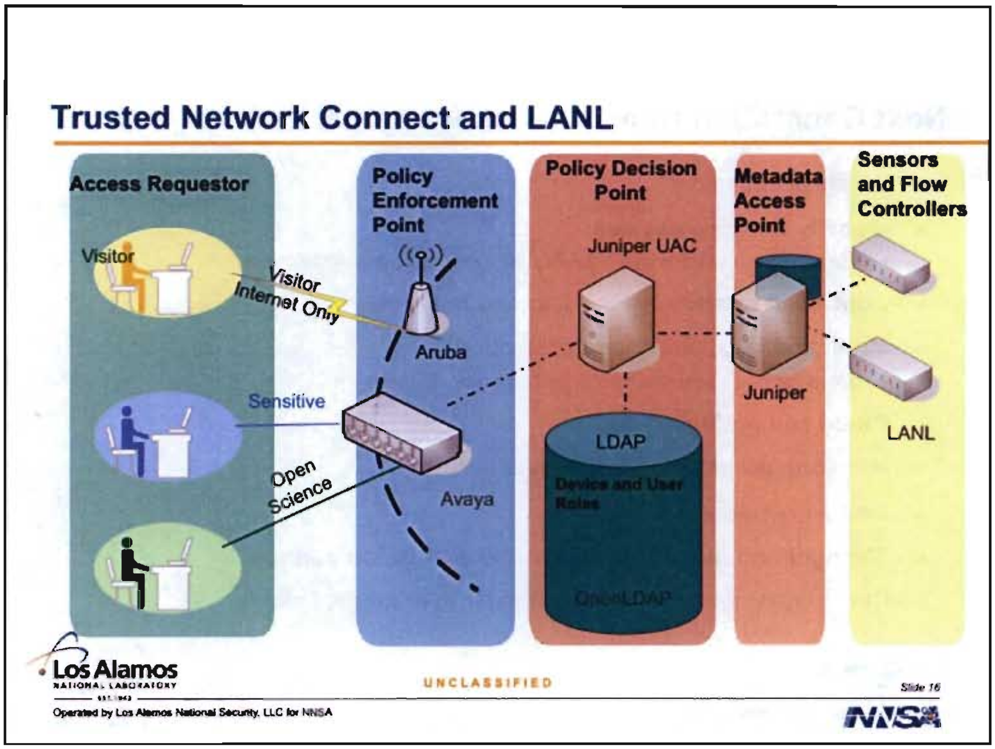
Slide 15

Operated by Los Alamos National Security, LLC for NNSA

NNSA

New requirements are not only about supporting new technology which is hard enough. It also means rethinking old policies and implementing them for new devices/OSes/access methods.

Some collaborations are asking for multi-site, multi-organization enclaves. Multi-site high performance computing and light water reactor research are 2 examples. Industry standards reduce the politics.



Trusted Network Connect and LANL

Access Requestor

Visitor

Visitor Internet Only

Sensitive

Open Science

Policy Enforcement Point

Aruba

Avaya

Policy Decision Point

Juniper UAC

LDAP

Device and User Roles

OpenLDAP

Metadata Access Point

Juniper

Sensors and Flow Controllers

LANL

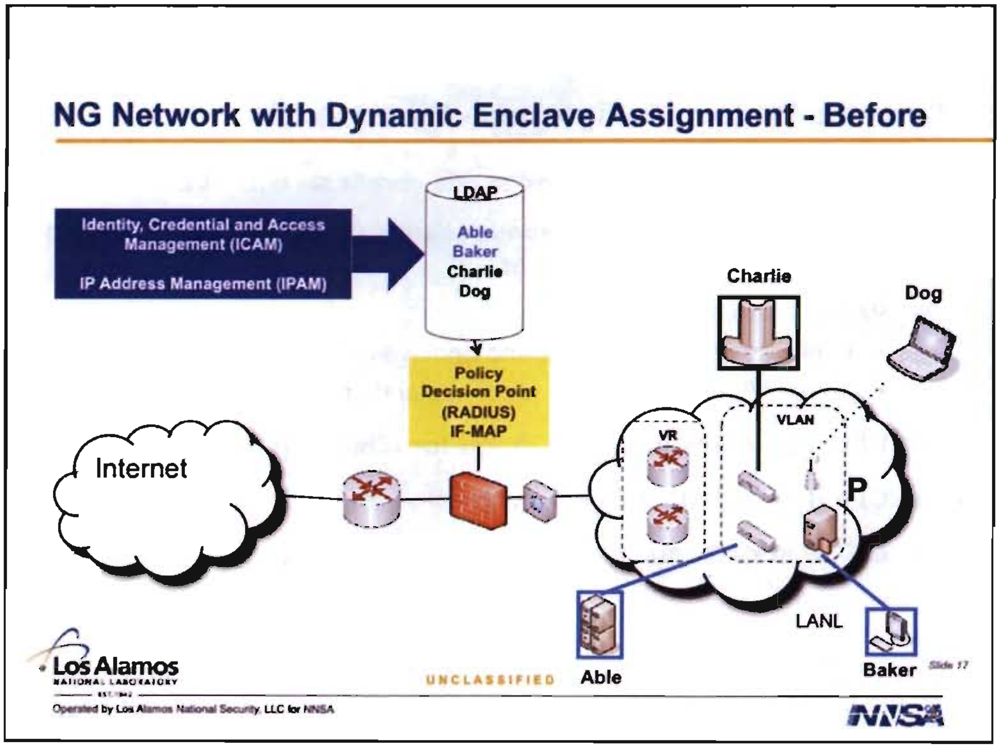
Los Alamos
NATIONAL LABORATORY
EST. 1943

UNCLASSIFIED

Slide 16

Operated by Los Alamos National Security, LLC for NNSA

NNSA



NG Network with Dynamic Enclave Assignment - Before

Identity, Credential and Access Management (ICAM)

IP Address Management (IPAM)

LDAP

Able
Baker
Charlie
Dog

Policy
Decision Point
(RADIUS)
IF-MAP

Internet

VR

VLAN

P

Charlie

Dog

LANL

Able

Baker

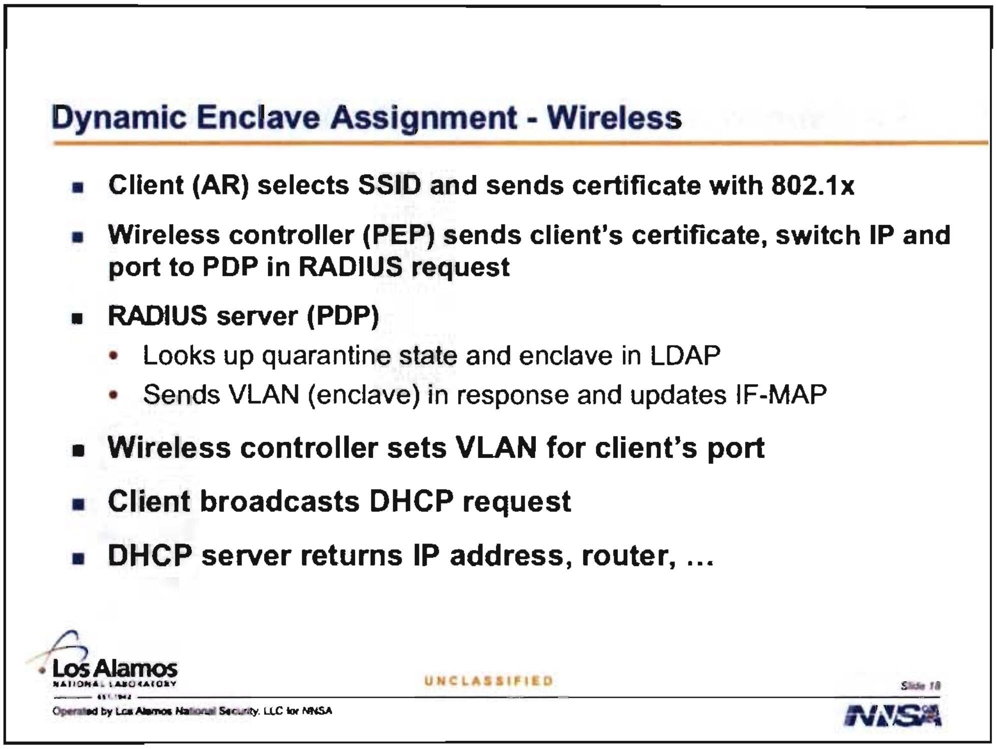
Los Alamos
NATIONAL LABORATORY
EST. 1943

UNCLASSIFIED

Slide 17

Operated by Los Alamos National Security, LLC for NNSA

NNSA



Dynamic Enclave Assignment - Wireless

- Client (AR) selects SSID and sends certificate with 802.1x
- Wireless controller (PEP) sends client's certificate, switch IP and port to PDP in RADIUS request
- RADIUS server (PDP)
  - Looks up quarantine state and enclave in LDAP
  - Sends VLAN (enclave) in response and updates IF-MAP
- Wireless controller sets VLAN for client's port
- Client broadcasts DHCP request
- DHCP server returns IP address, router, ...

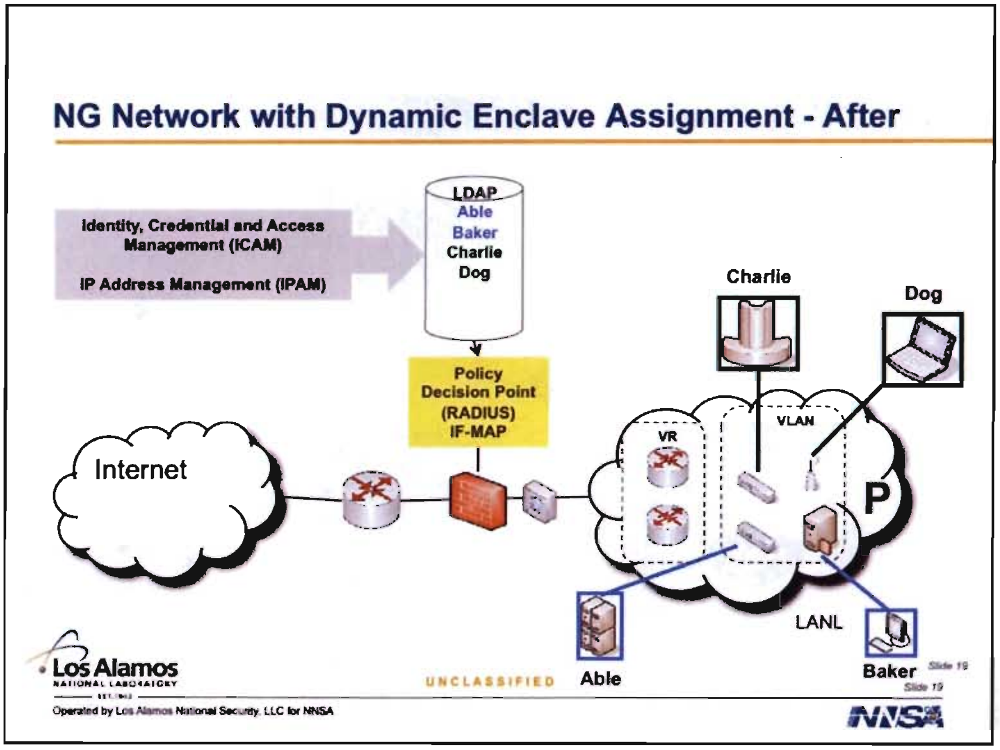
Los Alamos
NATIONAL LABORATORY
EST. 1943

UNCLASSIFIED

Slide 18

Operated by Los Alamos National Security, LLC for NNSA

NNSA



NG Network with Dynamic Enclave Assignment - After

Identity, Credential and Access Management (ICAM)

IP Address Management (IPAM)

LDAP
Able
Baker
Charlie
Dog

Policy
Decision Point
(RADIUS)
IF-MAP

UNCLASSIFIED

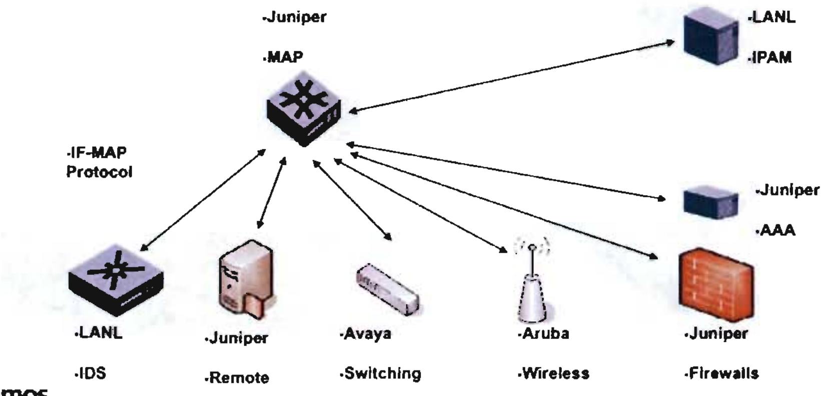
Slide 19

Los Alamos
NATIONAL LABORATORY
EST. 1943

Operated by Los Alamos National Security, LLC for NNSA

NNSA

TNC IF-MAP Coordinated Security



·Juniper

·MAP

·LANL

·IPAM

·IF-MAP Protocol

·Juniper

·AAA

·LANL

·IDS

·Juniper

·Remote

·Avaya

·Switching

·Aruba

·Wireless

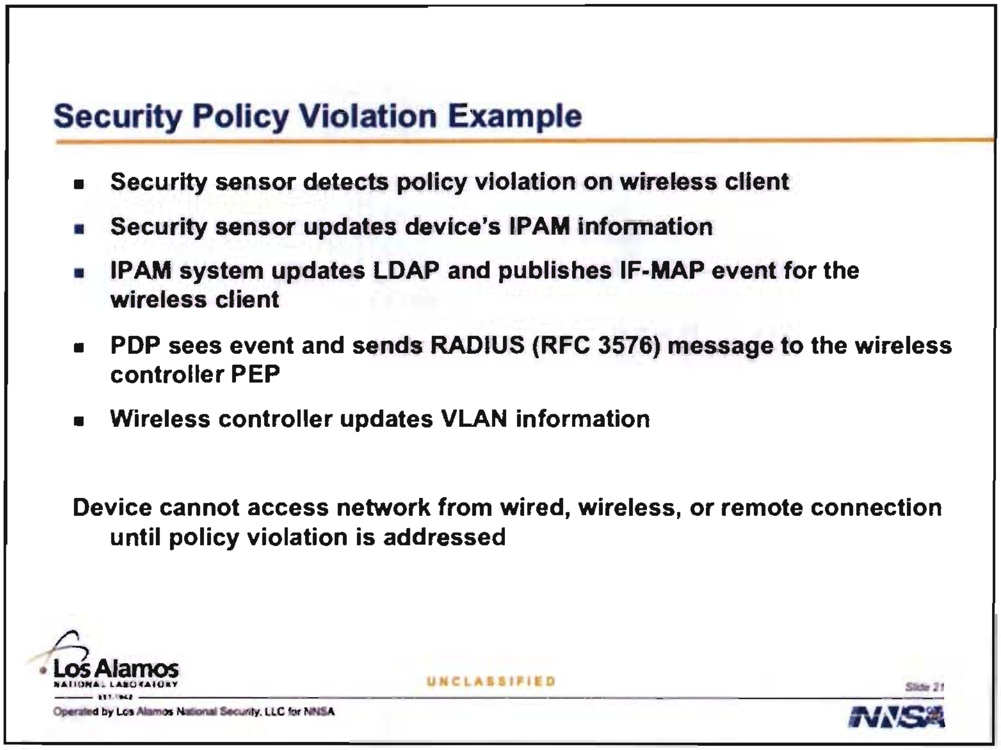
·Juniper

·Firewalls

Los Alamos NATIONAL LABORATORY EST. 1943

UNCLASSIFIED

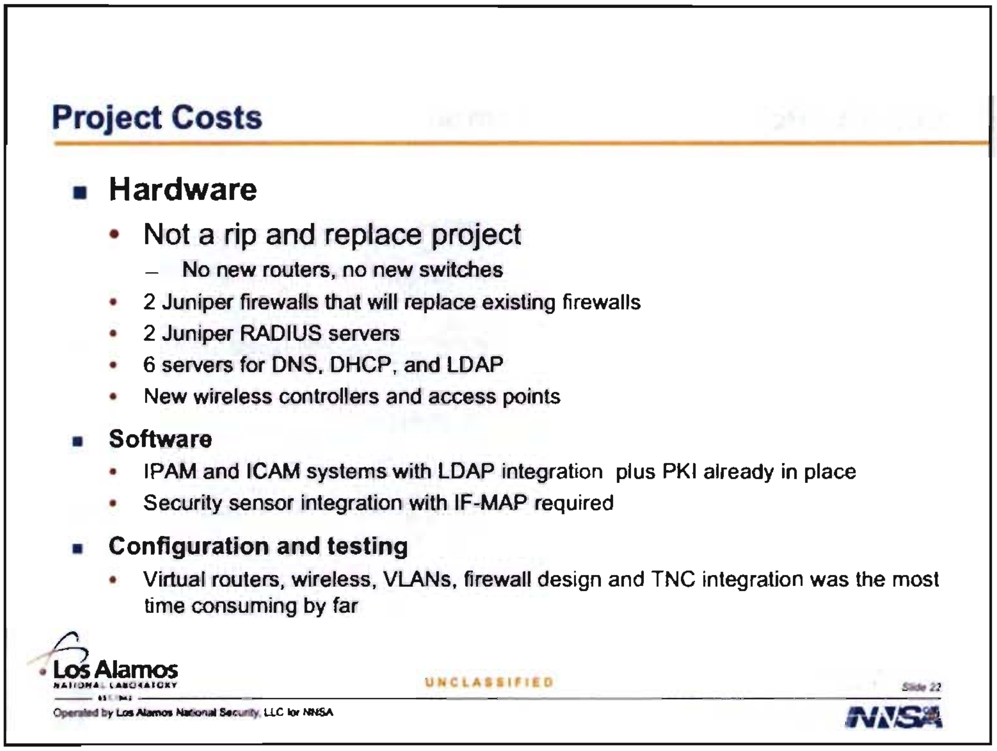
NNSA



Security Policy Violation Example

- Security sensor detects policy violation on wireless client
- Security sensor updates device's IPAM information
- IPAM system updates LDAP and publishes IF-MAP event for the wireless client
- PDP sees event and sends RADIUS (RFC 3576) message to the wireless controller PEP
- Wireless controller updates VLAN information

Device cannot access network from wired, wireless, or remote connection until policy violation is addressed



Project Costs

- **Hardware**
  - Not a rip and replace project
    - No new routers, no new switches
  - 2 Juniper firewalls that will replace existing firewalls
  - 2 Juniper RADIUS servers
  - 6 servers for DNS, DHCP, and LDAP
  - New wireless controllers and access points
- **Software**
  - IPAM and ICAM systems with LDAP integration plus PKI already in place
  - Security sensor integration with IF-MAP required
- **Configuration and testing**
  - Virtual routers, wireless, VLANs, firewall design and TNC integration was the most time consuming by far

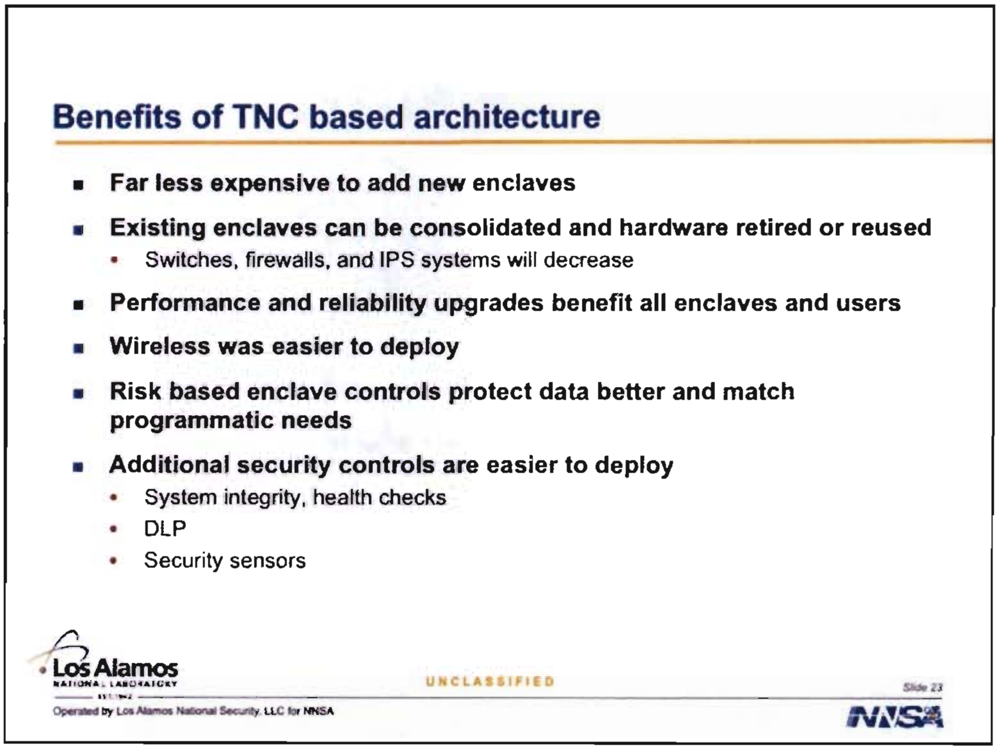
Los Alamos NATIONAL LABORATORY EST. 1943

UNCLASSIFIED

Slide 22

Operated by Los Alamos National Security, LLC for NNSA

NNSA



Benefits of TNC based architecture

- **Far less expensive to add new enclaves**
- **Existing enclaves can be consolidated and hardware retired or reused**
  - Switches, firewalls, and IPS systems will decrease
- **Performance and reliability upgrades benefit all enclaves and users**
- **Wireless was easier to deploy**
- **Risk based enclave controls protect data better and match programmatic needs**
- **Additional security controls are easier to deploy**
  - System integrity, health checks
  - DLP
  - Security sensors

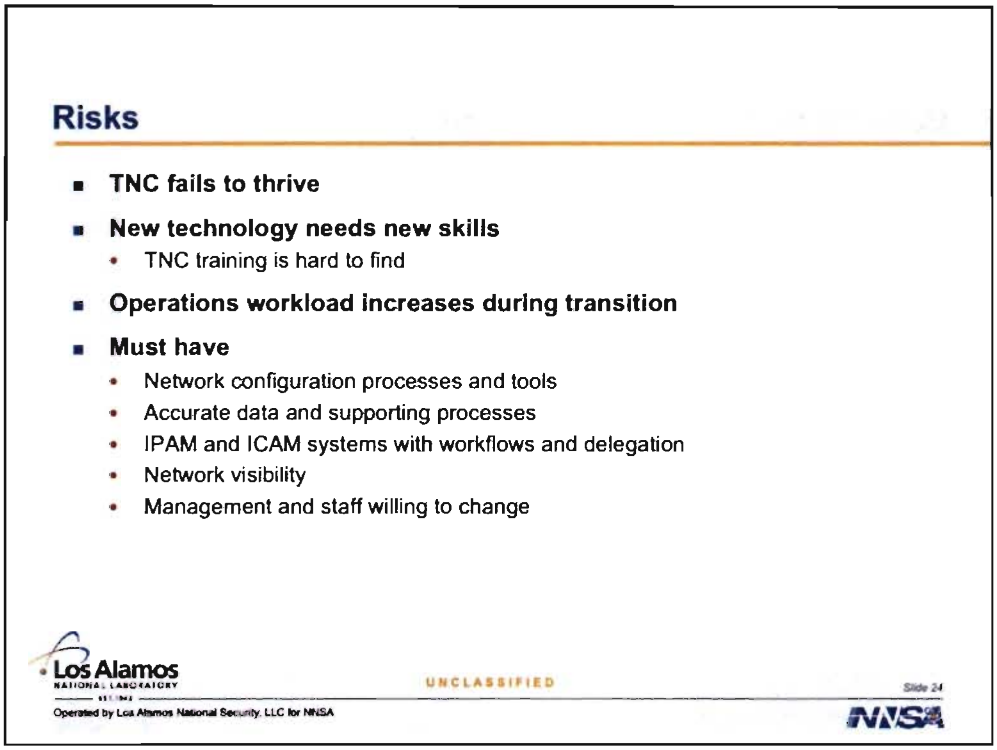
Los Alamos
NATIONAL LABORATORY
EST.1943

UNCLASSIFIED

Slide 23

Operated by Los Alamos National Security, LLC for NNSA

NNSA



Risks

- **TNC fails to thrive**
- **New technology needs new skills**
  - TNC training is hard to find
- **Operations workload increases during transition**
- **Must have**
  - Network configuration processes and tools
  - Accurate data and supporting processes
  - IPAM and ICAM systems with workflows and delegation
  - Network visibility
  - Management and staff willing to change

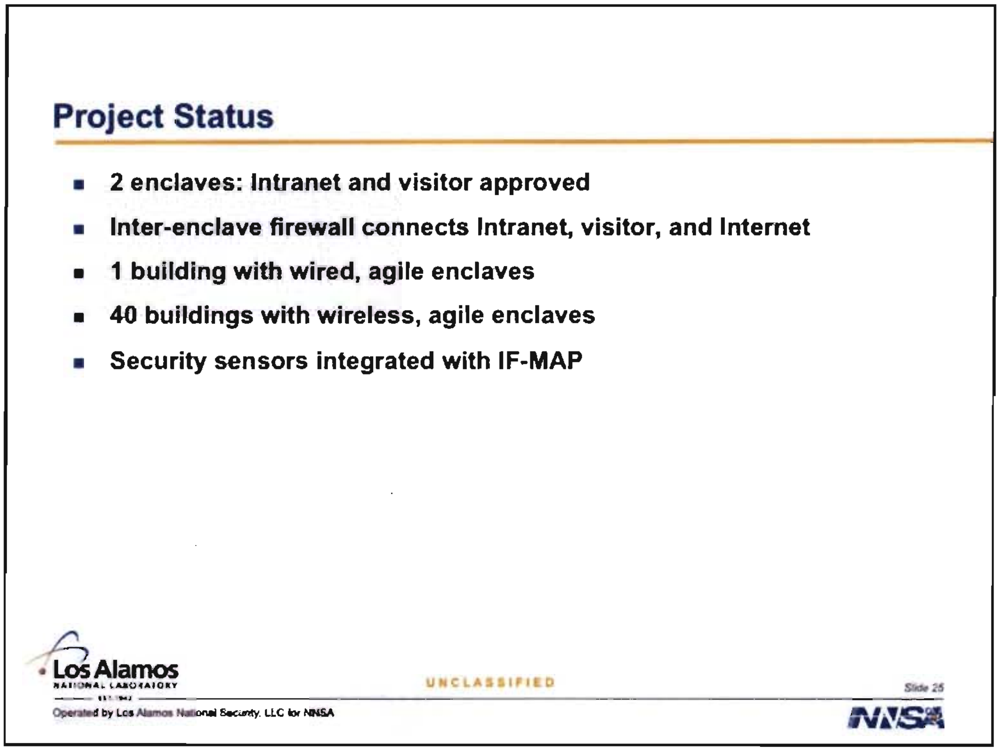
Los Alamos
NATIONAL LABORATORY
EST. 1943

UNCLASSIFIED

Slide 24

Operated by Los Alamos National Security, LLC for NNSA

NNSA



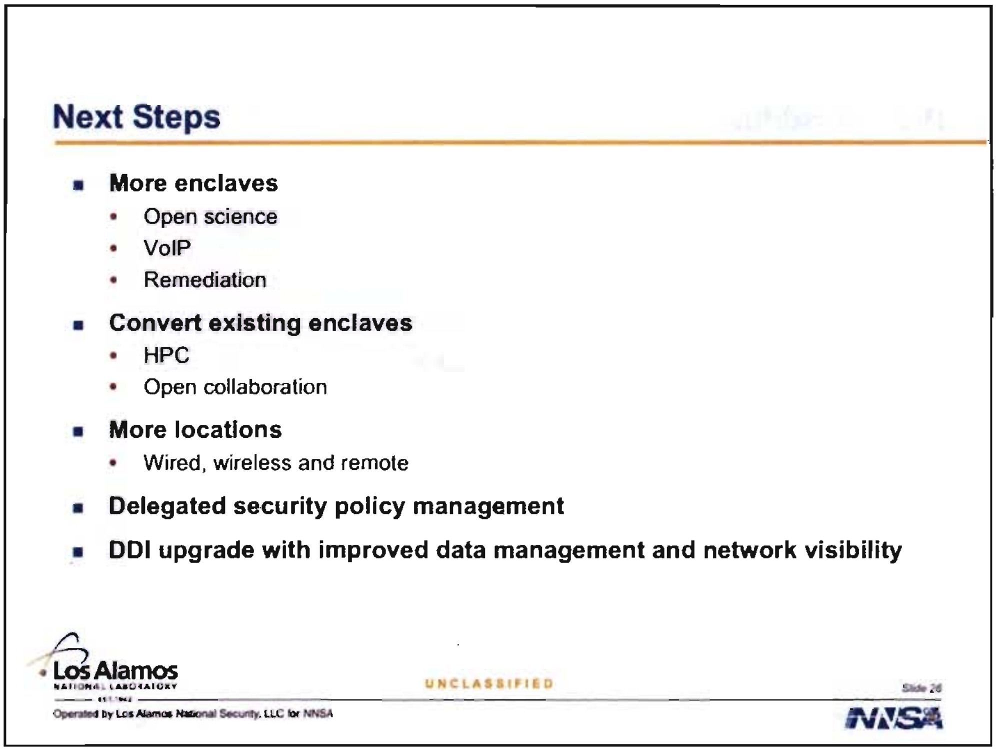
Project Status

- 2 enclaves: Intranet and visitor approved
- Inter-enclave firewall connects Intranet, visitor, and Internet
- 1 building with wired, agile enclaves
- 40 buildings with wireless, agile enclaves
- Security sensors integrated with IF-MAP

UNCLASSIFIED

Slide 25

Operated by Los Alamos National Security, LLC for NNSA



Next Steps

- **More enclaves**
  - Open science
  - VoIP
  - Remediation
- **Convert existing enclaves**
  - HPC
  - Open collaboration
- **More locations**
  - Wired, wireless and remote
- **Delegated security policy management**
- **DDI upgrade with improved data management and network visibility**

Los Alamos NATIONAL LABORATORY EST. 1943

UNCLASSIFIED

Slide 26

Operated by Los Alamos National Security, LLC for NNSA

NNSA