SAND2011-7421C

Lifecycle Management of Security Equipment and Infrastructure



Consuelo Silva
Sandia National Laboratories

November 2011

Discussion Overview

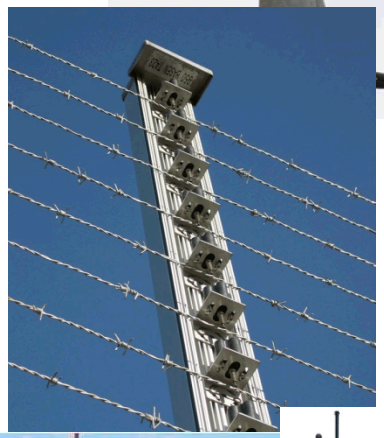
- Defense Nuclear Security (DNS) Program systems challenges
- Security infrastructure elements
- Lifecycle management benefits
- Lifecycle management planning
- Developing the DNS lifecycle management program
- Conditions assessments
- Preventative maintenance
- Performance testing
- Sustainment
- Summary

DNS Security System Challenges

- DNS security systems program suffered in the past – each site left to its own to manage the security systems portfolio
- Sites failed to invest in lifecycle replacement
  - Most sites had a "run to failure" approach for security systems
- Most sites did not have a comprehensive picture of the entire site-level security systems profile
- Security vulnerabilities associated with substandard systems were unknown
- Lifecycle planning was nonexistent
- NNSA inherited a large "mortgage" associated with the need to invest in complete replacement of security systems across all sites

Security Infrastructure Elements

- **Security infrastructure includes:**
  - Security posts – facility maintenance and repair
  - Perimeter intrusion detection and assessment systems
  - Command, control and communications systems
  - Primary and auxiliary power sources
  - Metal and explosive detection systems, x-ray machines and SNM monitors
  - Lighting systems
  - Fences, gates, doors and turnstiles
  - Interior intrusion detection systems
  - Biometric identification and badge reading systems
  - Protective forces equipment
  - Security vehicles

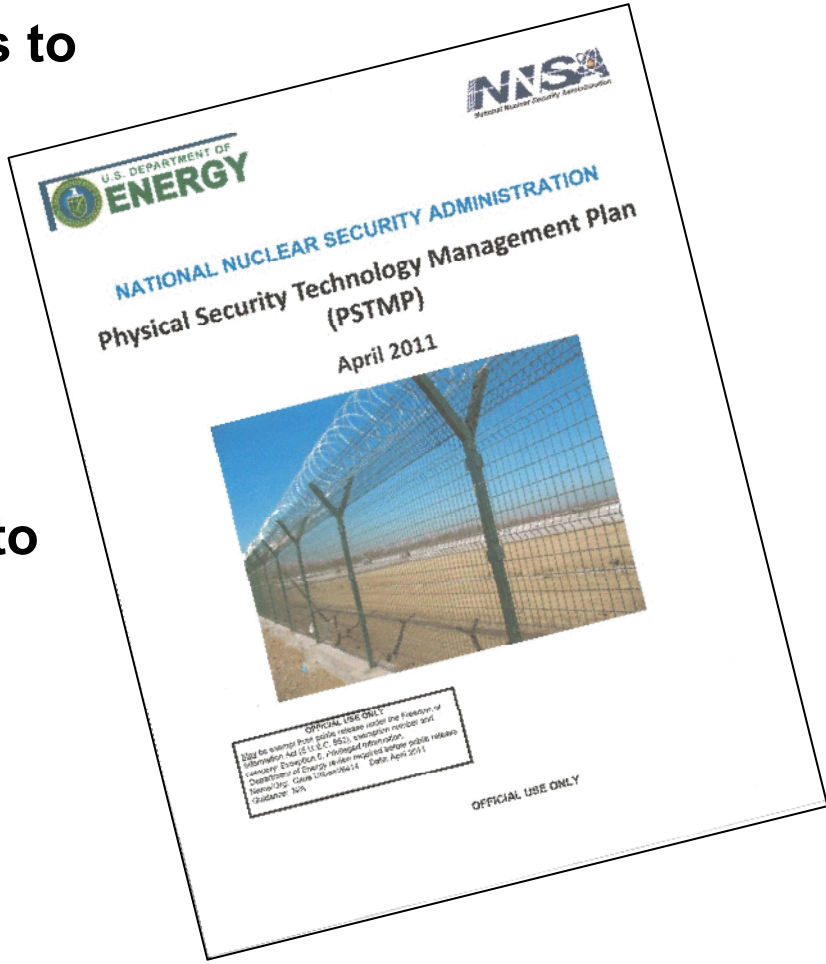


Lifecycle Management Benefits

- **Successful use of lifecycle management will:**
  - Identify current and future infrastructure needs
  - Identify potential problems, risks and constraints
  - Identify impacts of various courses of action
  - Influence preliminary designs for security facilities
  - Support strategic planning and budgeting for security infrastructure

Lifecycle Management Planning

- **Life-cycle management identifies costs to support security systems, including:**
  - **Planning**
  - **Operations**
  - **Testing and Maintenance**
  - **Replacement**
- **Understanding life-cycle costs is vital to strategic planning and budgeting**
  - **All costs are known and validated**
  - **Helps schedule expenditures**
  - **Identifies return on investment**



Developing the DNS Lifecycle Program

1-3 years

- Implement Process to Create Technology Management Plan
- Develop Complex-Wide NNSA & Site Relationships
- Collect Deployed Technology Data
- Conduct Technology Condition Assessments
- Security System Considerations Designed in from the Start

2-5 years

- Develop Complex-Wide Investment Strategies
- Make Complex-Wide Technology Deployment Decisions
- Create Budget Calls that include Lifecycle Components
- Security System Considerations Designed in from the Start

Out-years

- Maintain Lifecycle Budgeting for Technology Investments
- Implement Full Technology Standardization
- Maintain Complex-Centric Perspective
- Sustain Deployed Technology

Condition Assessment for Installed Systems

- **Development of a comprehensive listing of security infrastructure "elements" provides the foundation**
  - **Databases using "standard" descriptors is key to collecting useful data**
- **Use of vendor data is often not useful in predicting replacement frequency needs**
  - **Deployed operational conditions and maintenance attention drives repair and replacement needs**
- **Data-mining repair frequency can help identify systems in need of lifecycle replacement**
- **Comprehensive analysis and risk ranking is required to prioritize replacement schedules**

Security Systems Maintenance

- **Both preventive and corrective maintenance activities are vital to assuring high system effectiveness**
  - **Preventative maintenance is required to assure that critical security systems operate per requirements**
  - **Corrective actions are high priority for identified equipment**
  - **Compensatory measures are required until repairs are complete, performance is tested and the system/item is back in service**

Performance Testing Program

- **Testing can provide useful reliability and performance data to guide lifecycle replacement decisions**
- **Validation of security functions involves:**
  - **Operability testing**
  - **Performance testing reliability for:**
    - **New systems**
    - **Maintenance**
    - **Protective Force changes in operations**
- **Use of "two-person" testing capability to mitigate "insider" concerns**

Sustainment of the Lifecycle Program

- **Program sustainment has many related activities**
  - **Identification of appropriate requirements to meet operational requirements and security needs**
  - **Adequate and sustained funding is critical**
  - **Needs must be prioritized by balancing risk and available funding**
  - **Preventive and scheduled maintenance increases physical security systems life span and reduces life cycle infrastructure costs**

Summary

- Security systems provide a critical capability for nuclear security operations and must meet the highest possible reliability standards
- Lifecycle replacement programs require a comprehensive understanding of the installed systems and a formal management approach to ensure they meet the required performance standards
- DNS has developed and is implementing the Physical Security Technology Management plan that identifies, analyzes, plans for, funds, and replaces security infrastructure



QUESTIONS?