LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-CONF-412198

How to meet the NAPs and still have a life

L. K. Neely

April 15, 2009

DOE Cyber Security Conference
Henderson, NV, United States
May 11, 2009 through May 15, 2009

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Lawrence Livermore National Laboratory

How to meet the NAPs and still have a life:

LLNL Site Security Component Library

LLNL Security Plan Policy

May 13, 2009

Lee Neely

CISSP, MSP ISSO

Lawrence Livermore National Laboratory, P. O. Box 808, Livermore, CA 94551

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344

LLNL-CONF-412198

The Problem

Cyber Security Program
Office of the CIO

- Whether following NNSA Policy (NAP) 14.1-C,14.2-C, Department of Energy (DOE) 205.1-4, DOE 205.1-7 – all derive from National Institute of Standards and Technology (NIST) 800-53A controls
- Lots of details, lots of testing, lots of policy
- How to solve the problem and stay operational?

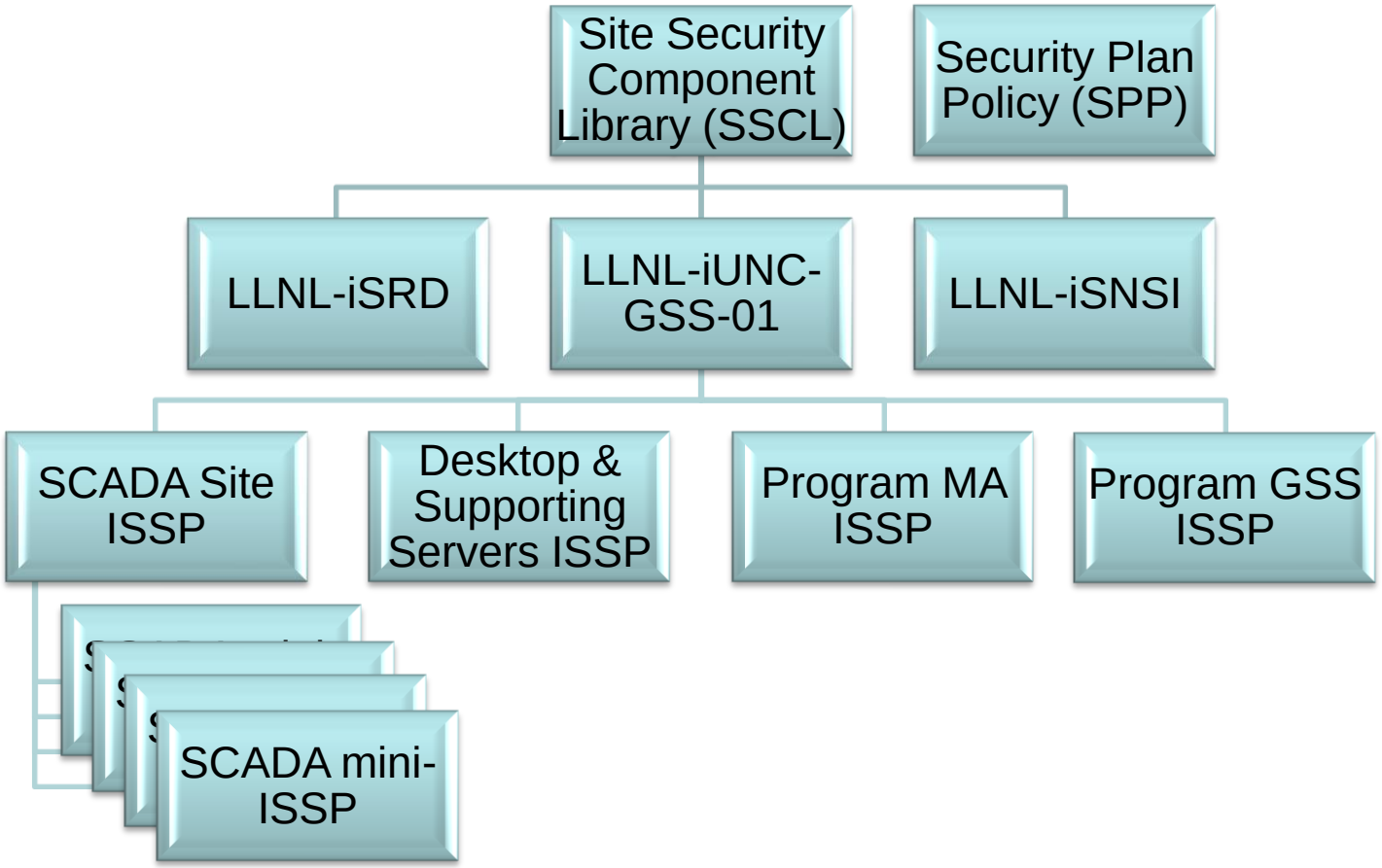
Keys to our success

Cyber Security Program
Office of the CIO

- Ah-ha moments:
  - Site Security Component Library (SSCL)
  - NAP Policy Document – Security Plan Policy (SPP)
- Success Factors
  - Use of “Core Services” – plans outsource to these
  - Separate the Supervisory Control and Data Acquisition (SCADA) systems
  - Leverage automation wherever possible
  - Partner with others – benefit from their experience
  - Continuity of Operations (COOP)/Business Impact Analysis (BIA) – follow FEMA model/processes

FY2009 LLNL ISSP plan hierarchy

Cyber Security Program
Office of the CIO



Site Security Component Library (SSCL)

Cyber Security Program
Office of the CIO

- NAPs require all components run a secure (known) pedigreed configuration
- At a site like LLNL there are many configurations, some necessary for mission objectives, others because “we can”
- The ah-ha moment:
  - Create a library, with configuration management, processes/etc. to record and document approved configurations
  - The number of entries is an IT decision, not a Cyber Security decision

SSCL Defined

Cyber Security Program
Office of the CIO

- Each library entry (configuration) includes
  - Description and pedigree (NIST, DISA, NSA, etc.)
  - Compliance testing script (SCAP, Perl, etc.) with repeatable verifiable results
  - List of NAP security controls met
  - Identification of deviations from pedigree and/or NAP requirements
  - Certification information
    - Who and when certified
      - If CSSM determines configuration outside current risk boundary, approval escalated to DAA

SSCL Defined

Cyber Security Program
Office of the CIO

- Process developed for submission, validation and maintenance of configurations
  - Updates could result in new library entries
    - Entry lifecycle needs to be decided
  - “Anyone” willing to follow the process can submit entry – allows for program needs and adjustment
  - Configurations could be derived from other entries

SSCL Acceptance

Cyber Security Program
Office of the CIO

- Process/oversight/buy-in
  - Develop Concept of Operations document
    - Present to management/others for buy-in
      - CIO, CSSM, DAA
    - Becomes base reference
  - Appoint project manager to implement the SSCL
  - Build SSCL team
    - SSCL Librarian
    - IT – technical expertise
    - Cyber Security – technical and security expertise
  - Build approval process

SSCL Library Implementation

Cyber Security Program
Office of the CIO

- Select a target to prototype the implementation
  - Run your first target to ground
- Build initial (subsequent) entries based on existing deployed configurations
  - Pedigree is key – where did it come from?
  - A good test that shows compliance with pedigree/library entry means a system is built to that specification
- Build database to record compliance
  - Ideally testing tools use automation to update
  - Report correlates with configuration management

SSCL Initial Library

Cyber Security Program
Office of the CIO

- LLNL initial SSCL entries:
  - Windows XP
  - OS X
  - Windows Server 2003
  - OS X Server
  - RHEL 4/5 Workstation
  - RHEL 5 Server

SSCL Compliance

Cyber Security Program
Office of the CIO

- SSCL Automation tools
  - Cross platform/cross technology
  - Run SCAP, other compliance testing scripts
  - Candidate solutions:
    - McAfee Policy Auditor
    - Tenable Security Center
    - LANDesk

SSCL Compliance

Cyber Security Program
Office of the CIO

- SSCL Testing
  - Compliance validation (CM-6) scripts run by program/IT staff as frequently as required to maintain compliance – may click “fix problems”
  - Compliance validation audit scripts run by Certification Agent (read-only) to ensure on-going compliance – no changes possible
- SSCL Reporting
  - Tool test results will be combined with LLNL Configuration Management Database (CMDB) asset information
  - Report by FISMA system planned

NAP Policy – Security Plan Policy (SPP)

Cyber Security Program
Office of the CIO

- Each control can be converted to a policy & procedure
  - Policy is simple and straight forward
  - Creates a single reference for policy and procedure
  - Policy answers the question of “Where is it written”
- Create a standard or default procedure to meet each control.
  - First implementation or procedure is the institutional answer
  - Programs may elect to create a different procedure
    - Both institutional and program procedure follow same approval process

NAP Policy – SPP Wins

Cyber Security Program
Office of the CIO

- Simplifies security plan submission
  - Individual security plan only includes security control information when NOT using institutional answer
  - Control implementation library and policy shared with DAA for approval and buy-in
- Security Testing
  - System will be tested against institutional or local implementation for each control
  - Working from a common (institutional) library, testing is known and simplified due to familiarity

NAP Policy – SPP Implementation

Cyber Security Program
Office of the CIO

- Possible to be bogged down in process for wide acceptance.
- Start simple
  - Start with easy control families – AT, AU, PS
  - Involve IT staff for implementation/procedure
  - Some controls are “free” or “dictated”
    - Personnel policy (screening/hiring/clearance)
    - Physical protections (guns/guards/gates)
    - Procurement policy
    - Information Security and Classification
  - Core services implement some controls for all

Core Services

Cyber Security Program
Office of the CIO

- Core services developed for common answers to controls
- Core services meet certain NAP controls
  - Systems subscribing to those services get associated controls for “free” – no additional paperwork
  - Core services aid common solution delivery

Core services for LLNL Institutional Unclassified (iUNC) ISSP

Cyber Security Program
Office of the CIO

- 5ESS
- Access account management
- Active Directory
- Blue Network Infrastructure
- Blue Coat (Web Proxy)
- CMDB
- Captive Portal Network
- DNS
- Email w/security services
- Encase
- Entrust PKI
- EOR
- Firewall
- Green Collaboration Environment
- ICS Audio/Web Conferencing
- Identity Management
- Intrusion Detection System (IDS)
- Institutional Instant Messaging (IIM)
- OS Imaging/Installation
- Intrusion Prevention System (IPS)
- IPSec VPN
- IP Telecom Services
- IT Service Management
- LANDesk
- MS (AD) PKI
- Network Time
- Open Terminal Service (OTS)
- PAC Management
- Red Hat Network (RHN)
- Routers & Switches
- SAV
- SSL VPN
- Two-Factor authentication
- Vulnerability Scanning
- Wireless
- Wireless IDS

SCADA Systems

Cyber Security Program
Office of the CIO

- DOE has SCADA guidelines
- NIST 800-82 defines SCADA controls
  - Cannot operate like common computers
  - Often isolated and/or protected
  - Often run-to-failure OS or components
    - Update/upgrade usually very expensive
- Developed a single Site Plan for SCADA systems
  - Developed mini-ISSP for each SCADA system

Automation

Cyber Security Program
Office of the CIO

- Automate and centralize as much as possible
  - Tools feed data to CMDB and Data Warehouse for reporting
  - User provisioning (IdM) tied to badge issuance/revocation
  - IdM feeds Active Directory, LDAP, Oracle OID and other sources of authentication
  - Manage passwords from central controls for consistency
  - Centralized ingress/egress/proxy controls, with one deviation management process.

Automation (cont)

Cyber Security Program
Office of the CIO

- Site license automation tools to achieve common solutions:
  - SPLUNK for audit log reduction, reporting and retention
  - Tenable Security Center to view vulnerabilities
  - LANDesk (IT users)
    - SCAP and custom compliance checks and fixes
    - Patch deployment and validation
  - McAfee Policy Auditor (C&A users)
    - to view configuration compliance (C &A users)
- ➢ Separate your IT and your certification automation tools.

Partner with others

Cyber Security Program
Office of the CIO

- DOE-CIRC
  - External web application scanning/testing
  - Network traffic monitoring/anomaly detection
- DOE enterprise licenses
  - McAfee Policy Auditor
  - ISS
  - Etc.
- Other Labs
  - Find someone similar and leverage their answers
- Other agencies
  - FEMA COOP/BIA planning/templates

FEMA COOP/BIA

Cyber Security Program
Office of the CIO

- Use FEMA model for contingency planning and recovery
  - Core services tiered based on this model
  - Each core service has a BIA/COOP plan
  - Each ISSP has a BIA/COOP plan
  - These build to site IT BIA/COOP plan
- LLNL emergency management already expert in COOP
  - Expert in physical COOP processes
  - Learning to be expert in IT COOP processes
  - Use of joint table-top exercises very educational

Where are we?

Cyber Security Program
Office of the CIO

- iUNC plan submitted to DAA
- First SCADA sub-plan submitted to DAA (“Astro” – LLNL trunked radio system)
- LLNL SPP submitted to LLNL CIO policy board
- Cyber Security Program learning to say how rather than yes or no

What's Next?

Cyber Security Program
Office of the CIO

- Waiting for DAA response to submitted plans
- Populate SSCL with configurations
- Implement McAfee Policy Auditor
- Policy board approvals
- Management agreement with institutional/local controls

Questions?

Cyber Security Program
Office of the CIO

My contact information:

Email: neely1@llnl.gov

Phone: (925) 422-0140