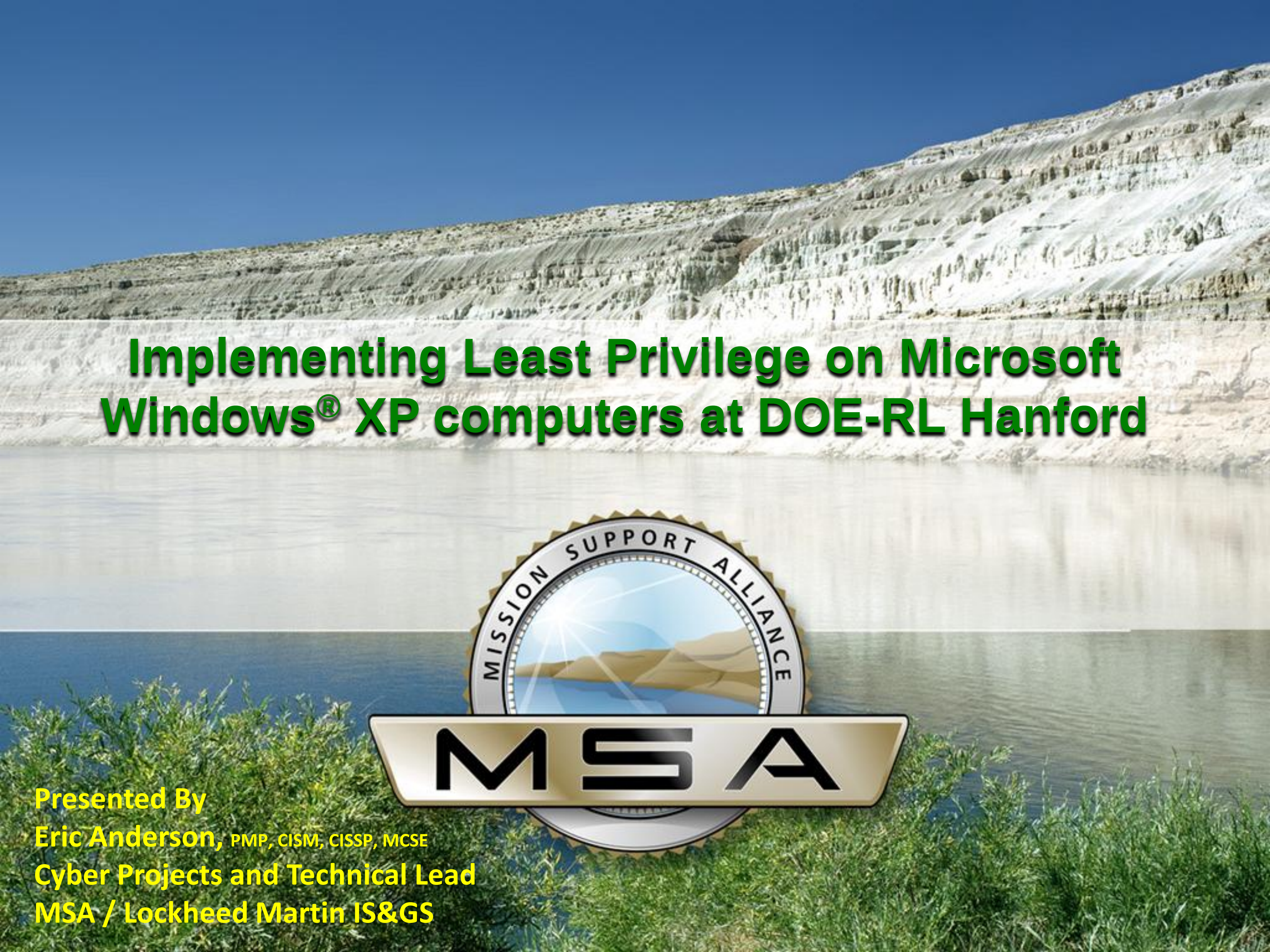


Implementing Least Privilege on Microsoft Windows® XP computers at DOE-RL Hanford

MISSION SUPPORT ALLIANCE

MSA

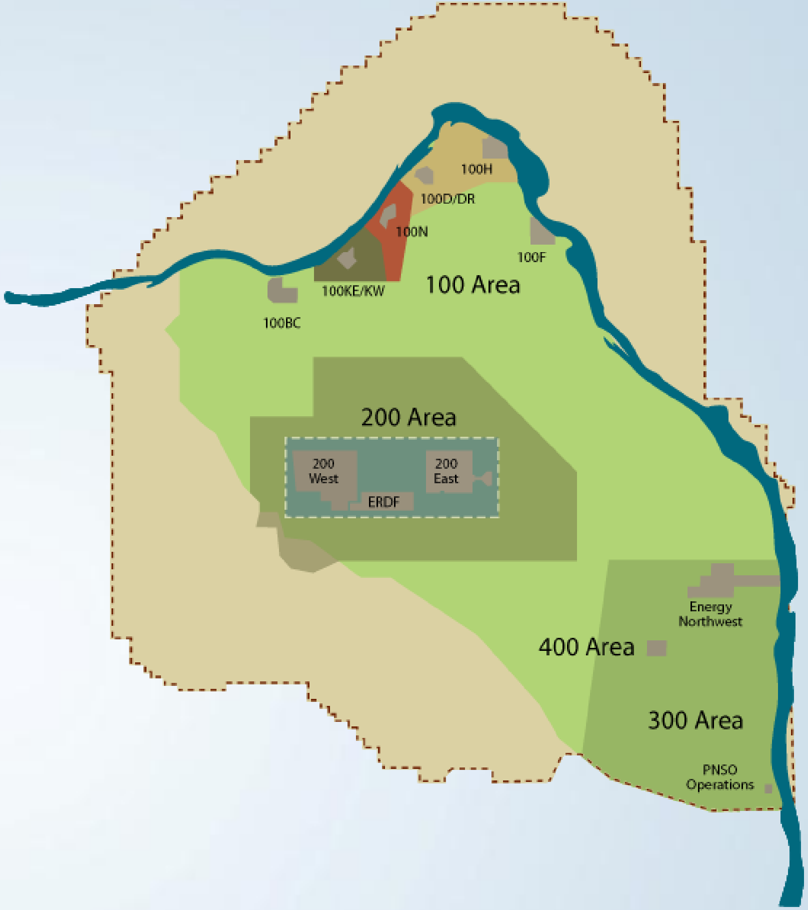
Presented By
Eric Anderson, PMP, CISM, CISSP, MCSE
Cyber Projects and Technical Lead
MSA / Lockheed Martin IS&GS

DOE Hanford Site

“To make our customers extraordinarily successful in our unified mission of cleaning up the Hanford Site…”

Hanford Site Scope

- 586 square miles
- 9,000+ PCs
- 500+ servers
- 400+ applications
- 1,000+ miles fiber to 300 bldgs
- 12,500+ phones



What’s the problem?

Compliance problem –

- OIG finding in 2007 … too many users operate as a “privileged,” **Local Administrator (LA)** on their computers.

Cyber Security problem –

- Users engage in risky activities while operating as LA.
- 68% of the 6,800 computers at DOE-RL (June 2008) ran with LA.

IT Administration problem –

- Difficult to upgrade from Windows® XP to Windows® 7 without getting client privilege usage under control.

Least Privilege

Microsoft recommends use of least-privileged user accounts (LUA)

“The LUA approach ensures that users follow the principle of least privilege and always log on with limited user accounts.“

Applying the Principle of Least Privilege to User Accounts on Windows® XP
Published: January 18, 2006. http://technet.microsoft.com/en-us/library/bb456992.aspx

User Account Control (UAC)

Microsoft defaults to User Account Control (UAC) in Windows® 7

“User Account Control is a security feature in Windows® 7 that was introduced with Windows Vista.”

“The primary goal of User Account Control is to reduce the exposure and attack surface of the Windows® 7 operating system by requiring that all users run in standard user mode, and by limiting administrator-level access to authorized processes.”

“By default, Windows® 7 runs every application as a standard user even if the current user is logged on as a member of the Administrators group.“

Least Privilege, User Account Control, and Setuid

http://technet.microsoft.com/en-us/library/cc770863.aspx

Why not remove all LA's?

Some applications are not developed or configured to use "least privilege."

Therefore, removing LA impacts the use of some applications that users need to do their jobs and to satisfy mission goals.

4 Categories of Users Run as LA

Experience from the field …

1. Most users do not need to run as LA
2. Administrators need LA to troubleshoot
3. Small number of users (~100) need “persistent” LA
4. Sometimes users (average ~60/day) need “temporary” LA

What’s the approach or PLAN
… for reducing the number of LA’s?

Scenario 1 – Remove users as LA on all computers, fix all breakage.

Scenario 2 – Fix all critical & essential applications needing LA to install and run, then remove all LA’s and fix breakage.

Scenario 3 – Implement a “white list” product to discover applications with LA dependencies, remove all LA’s and fix remaining breakage.

Scenario 4 – Identify and fix all applications needing LA to install and run, then remove all LA’s and fix breakage.

What's needed to implement the PLAN?

Need a Local Administrator Reduction Project (LARP) to quickly & effectively reduce LA on Windows XP computers

- Identify applications that are dependent on LA to install or run.
- Fix or remediate the LA-dependent applications.
- Remove LA privileges from all site computers, and
- Implement controls to keep LA privileges removed unless the need is justified and authorized.

LARP is Phase 1 of the 2-phased approach.

Next Steps … Identify key stakeholders potentially impacted by LARP project

- Senior management
- Application owners
- Product managers
- Application and system administrators
- Software developers & testers
- Service Desk (or Customer Technical Support)
- General users

LARP Project Activities

Application Management

- Take inventory
- Test for install without LA
- Test for execution without LA
- Fix or remediate LA-dependent applications

Privilege Management

- Develop or procure a privilege elevation tool
- Register “legitimate” LA usage
- Control “legitimate” LA usage
- Report on LA usage frequency for computers & users
- Document risk acceptance for “legitimate” LA usage

What were important TOOLS?

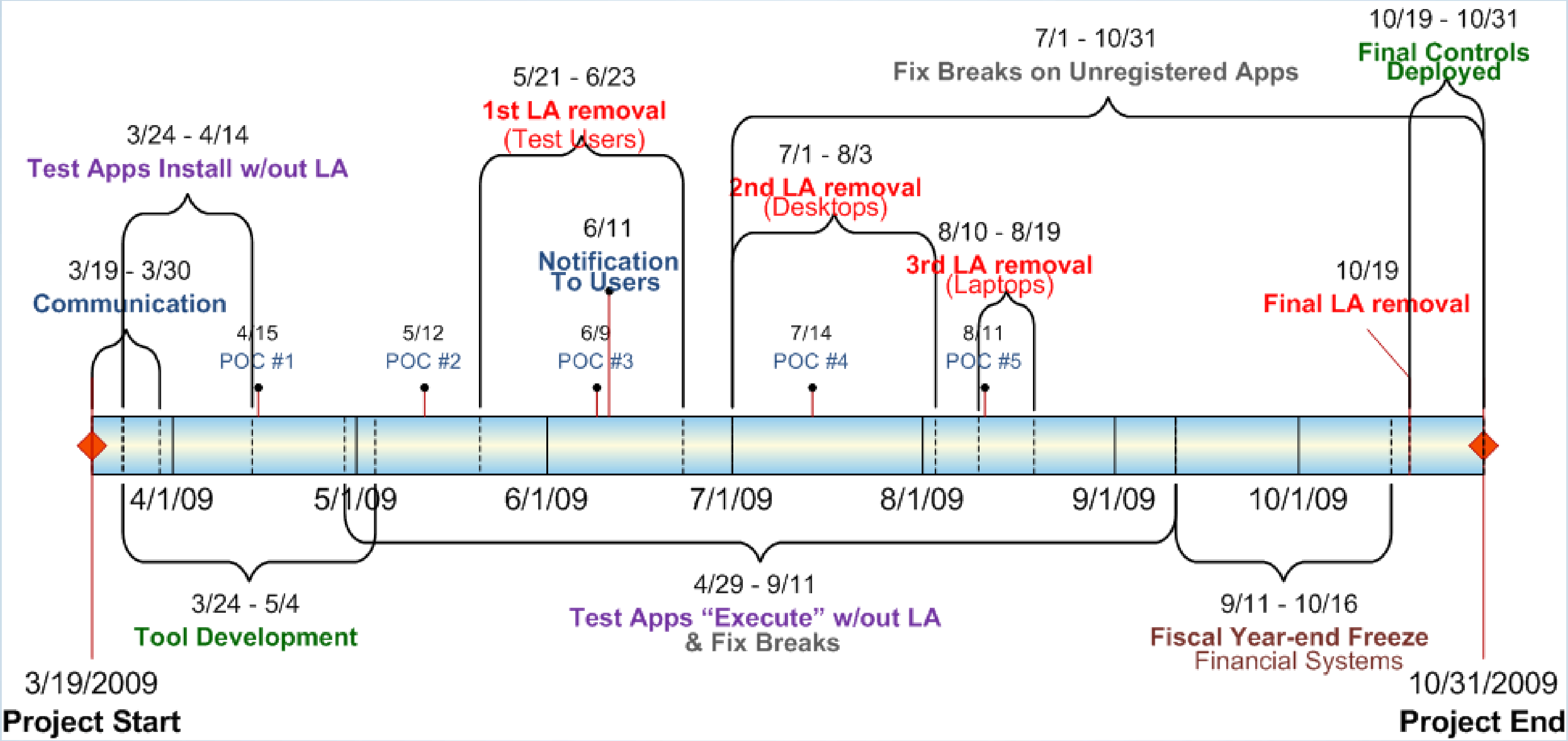
Experience from the field …

1. **Application Inventory * -** to identify all applications to test.
2. **LARP SharePoint site -** for project, tester, help desk and user communication.
3. **LARP mailbox -** for the project to respond to specific troubleshooting requests.
4. **Software distribution system * -** for the site to fix/remediate LA install issues.
5. **Microsoft® Systems Management Server -** (**SMS**) for application inventory assistance.
6. **Privilege elevation tool * -** (set Local Administrator, or **setLA)** for testers and general users.
7. **Account Management System * -** (**AMS**) to register legitimate LA usage.
8. **Network system logon process * -** (**Syslogon**) to control legitimate LA usage.
9. **Local Group Machine Enumeration * -** (**LGME**) reports "potential" for administrative access.
10. **Metric reporting * -** from backend information system databases (Syslogon, setLA & LGME).

* Denotes Hanford Local Area Network (HLAN) custom tools or systems.

Schedule of Activities

Experience from the field …



Application Management

Why take inventory?

- Application inventory provides a:
  - Good baseline for estimating project costs;
  - Assessment of impacts to users; and
  - Tracking outcomes of test\mitigation activities.

- It's a critical security control to know which software or applications are authorized to run on network computers, and which are not.

  SANS Consensus Audit Guidelines, 20 Critical Controls for Effective Cyber Security, http://www.sans.org/critical-security-controls/

Application Management

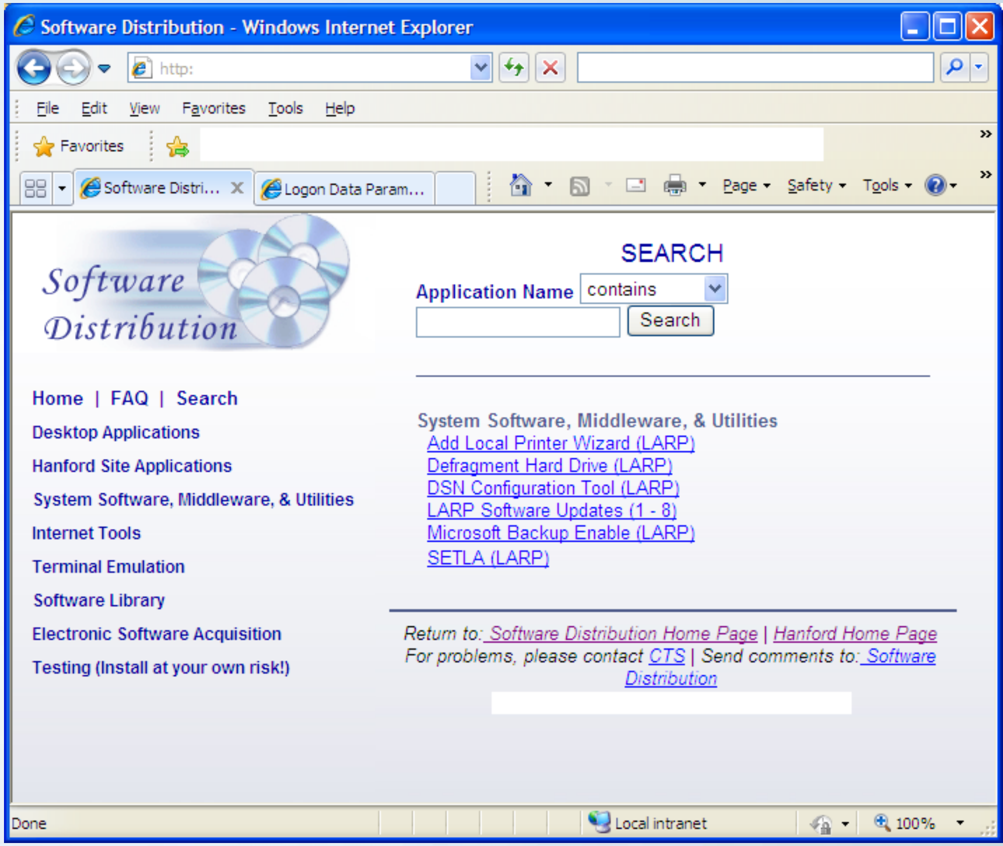
Test for install and execute without LA

- Test whether application installation requires LA privileges
  - easily handled by one person.
- Test whether application execution requires LA privileges
  - usually many people (system owner, application support or users).

Application Management

Fix / Remediate application dependence on LA

- Move all software installs to a site software distribution method to enforce configuration management, develop install tools or wizards, or both (below).
- Change permissions on directories, registry keys or files for applications needing LA to execute.



Software Distribution

SEARCH

Application Name contains

Search

Home | FAQ | Search

Desktop Applications

Hanford Site Applications

System Software, Middleware, & Utilities

Internet Tools

Terminal Emulation

Software Library

Electronic Software Acquisition

Testing (Install at your own risk!)

System Software, Middleware, & Utilities

- Add Local Printer Wizard (LARP)
- Defragment Hard Drive (LARP)
- DSN Configuration Tool (LARP)
- LARP Software Updates (1 - 8)
- Microsoft Backup Enable (LARP)
- SETLA (LARP)

Return to: Software Distribution Home Page | Hanford Home Page

For problems, please contact CTS | Send comments to: Software Distribution

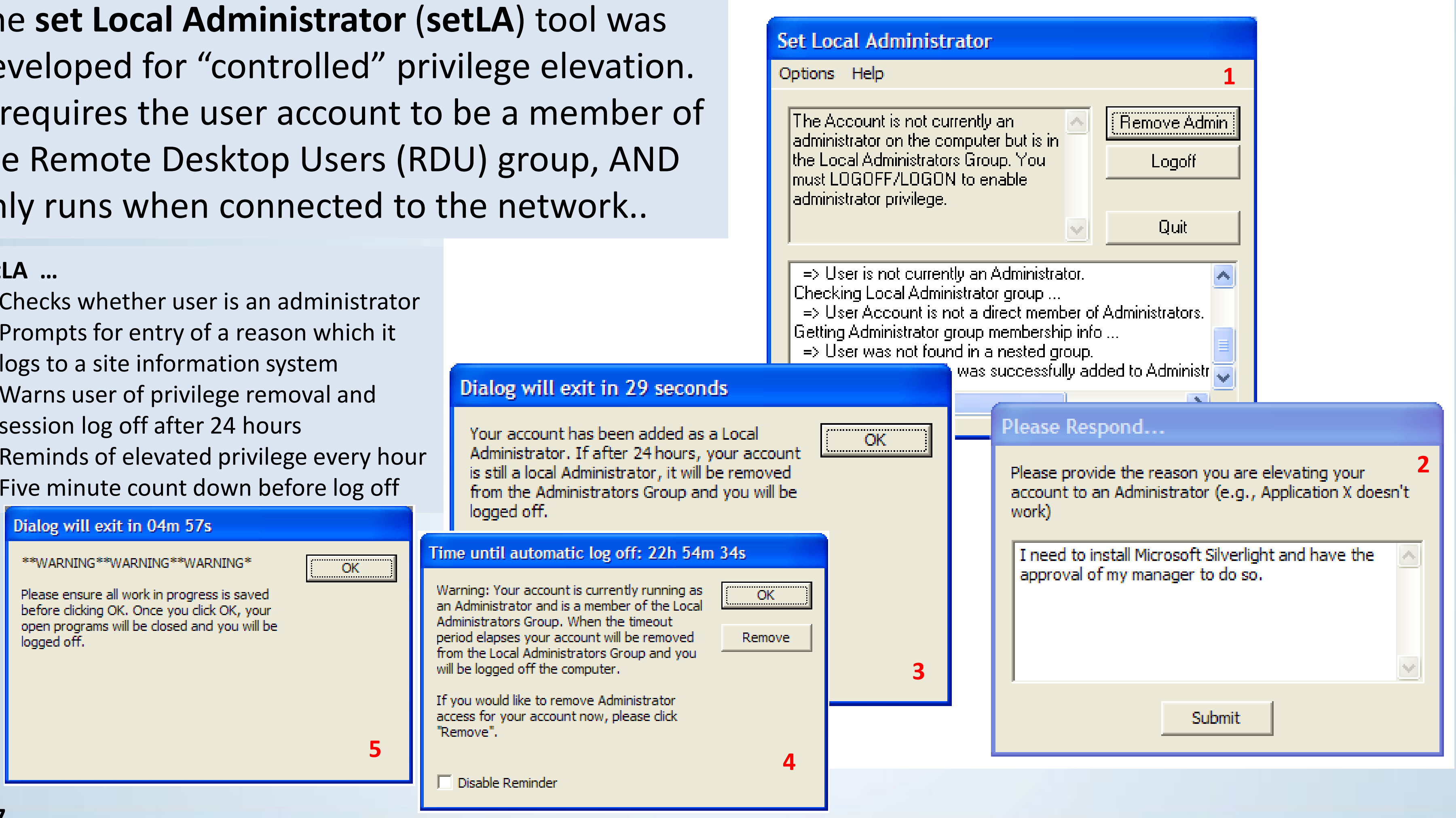
Privilege Management

Privilege elevation “setLA” tool

The **set Local Administrator** (**setLA**) tool was developed for “controlled” privilege elevation. It requires the user account to be a member of the Remote Desktop Users (RDU) group, AND only runs when connected to the network..

SetLA …

1. Checks whether user is an administrator
2. Prompts for entry of a reason which it logs to a site information system
3. Warns user of privilege removal and session log off after 24 hours
4. Reminds of elevated privilege every hour
5. Five minute count down before log off



Set Local Administrator

The Account is not currently an administrator on the computer but is in the Local Administrators Group. You must LOGOFF/LOGON to enable administrator privilege.

```
  => User is not currently an Administrator.
Checking Local Administrator group ...
  => User Account is not a direct member of Administrators.
Getting Administrator group membership info ...
  => User was not found in a nested group.
was successfully added to Administr
```

Please Respond...

Please provide the reason you are elevating your account to an Administrator (e.g., Application X doesn't work)

I need to install Microsoft Silverlight and have the approval of my manager to do so.

Dialog will exit in 29 seconds

Your account has been added as a Local Administrator. If after 24 hours, your account is still a local Administrator, it will be removed from the Administrators Group and you will be logged off.

Time until automatic log off: 22h 54m 34s

Warning: Your account is currently running as an Administrator and is a member of the Local Administrators Group. When the timeout period elapses your account will be removed from the Local Administrators Group and you will be logged off the computer.

If you would like to remove Administrator access for your account now, please click "Remove".

☐ Disable Reminder

Dialog will exit in 04m 57s

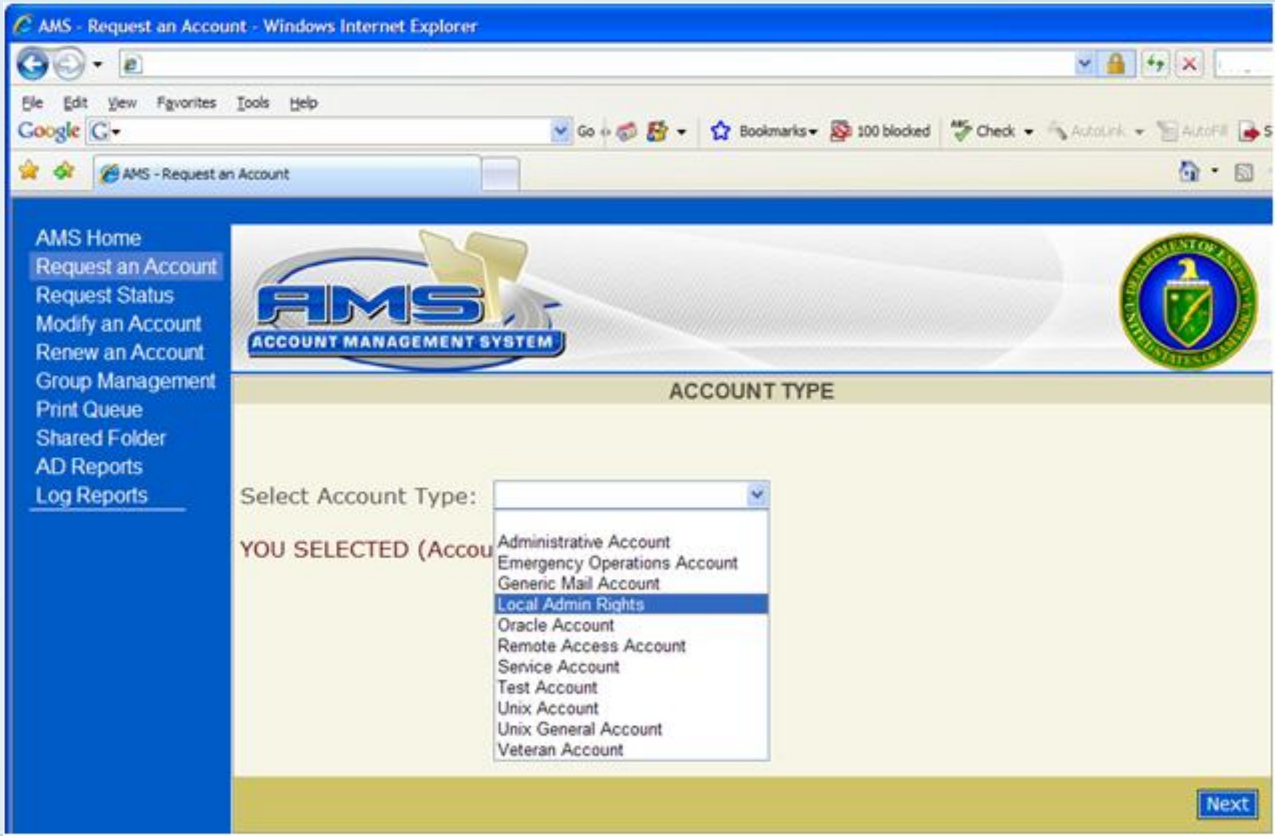
WARNINGWARNING**WARNING*

Please ensure all work in progress is saved before clicking OK. Once you click OK, your open programs will be closed and you will be logged off.

Privilege Management

Register "persistent" LA usage

- Site Account Management System (AMS) modified to register and authorize each user needing persistent LA rights to a specific computer.
- AMS registrations are reauthorized on an annual basis.



ACCOUNT TYPE

Select Account Type:

- Administrative Account
- Emergency Operations Account
- Generic Mail Account
- Local Admin Rights
- Oracle Account
- Remote Access Account
- Service Account
- Test Account
- Unix Account
- Unix General Account
- Veteran Account

YOU SELECTED (Accou

Privilege Management

Control "legitimate" LA usage

- Syslogon process controls LA privileged use at network logon.
- Enforces removal of all user accounts in Local Administrators group of Windows® XP computers not registered in the Account Management System (AMS).

Privilege Management

Reporting on LA usage for computers & users

- Syslogon process audits to an information system database.
- SetLA tool audits privilege elevation events to a system database.
- Auditing is enabled on Windows® XP computer security event logs for privilege escalation occurrences.
- All Windows® XP computer event logs are collected to a site SIEM.
- Local Group Machine Enumeration (LGME) runs periodically to ***assess potential of nested domain group membership*** in the Local Administrator group of the Windows® XP computer, and audits to a system database.

Privilege Management

Document legitimate LA usage

- Annual justification of persistent LA usage is required for user accounts and groups.
- Cyber risks of persistent LA usage is reassessed periodically for acceptance by the site DAA.

Completion of Controls
Phase 2

- **All membership** in the LA group of the client computer by local or domain accounts, or domain groups **must be registered** to AMS, and **controlled** by members of the domain Support group, their delegates or domain group policy.
- **Control** the **membership** of domain groups added to the LA group.
- **Local user accounts** as LA **reduced** to the least number possible and **actively monitored**.
- **Monitor** setLA privilege elevation usage and **limit** to a set number per-user per-period, or else an AMS justification required.
- Goal is **upgrade to Windows® 7** with User Account Control (UAC).

“Gotchas” & Other Lessons Learned

- SetLA initially allowed any domain User to elevate their privilege to LA, whether it was their own computer or not. Since many users connect remotely to their computers, the Remote Desktop Users (RDU) group was adapted to manage privilege elevation.
- SetLA “time bomb” messages added warning of automatic log off.
- Laptops have special needs for LA use as compared to Desktops.

Big wins!

- Reduced attack surface of site computers.
- Protection from malware installs, unintentional file downloads and configuration changes.
- LARP project identified unregistered applications (additional 50%) and got them registered in the Software Inventory application.
- LARP helped tighten up computer configuration management. Users really have to go out of their way now to download and install unapproved software or make configuration changes on their Windows® XP computers.

Mission Accomplished

Before LARP Project:

~68% of all Windows® XP computers ran as LA.

After LARP Project (on any given day):

<6% of Windows® XP computers ran as LA, and
<4.5% of Hanford users ran as LA.

And our stakeholders didn’t kill us!!

Questions?

Eric Anderson
Ernest_A_Eric_Anderson@RL.GOV
Lockheed Martin