SAND2018-12150C

TITUS Email Marking Project Deployment Update

National Nuclear Security Administration

The Office of the Associate Administrator for Information Management and Chief Information Officer

Sandia National Laboratories

03/28/2018

Presenters Bio's

Mark Holtzclaw

Mark is the NNSA OCIO Project Manager for the TITUS deployment project. He works closely with the technical team that is handling the configuration of the TITUS software. Mark has over 35 years of IT experience. He supported Sandia National Labs for over 18 years, before becoming a Project Manager for the NNSA OCIO PMO (Project Management Office).

Mark Timms

Mark Timms is a project manager in the IT Enterprise Collaboration group at Sandia National Laboratories. Mark has been with Sandia for three years. He managed the team that implemented the Titus Email Classification tool for the Sandia Classified Network in Feb of 2017 and the Sandia Partner Network in June of 2017. Prior to working at Sandia, Mark worked at Intel for 17 years.
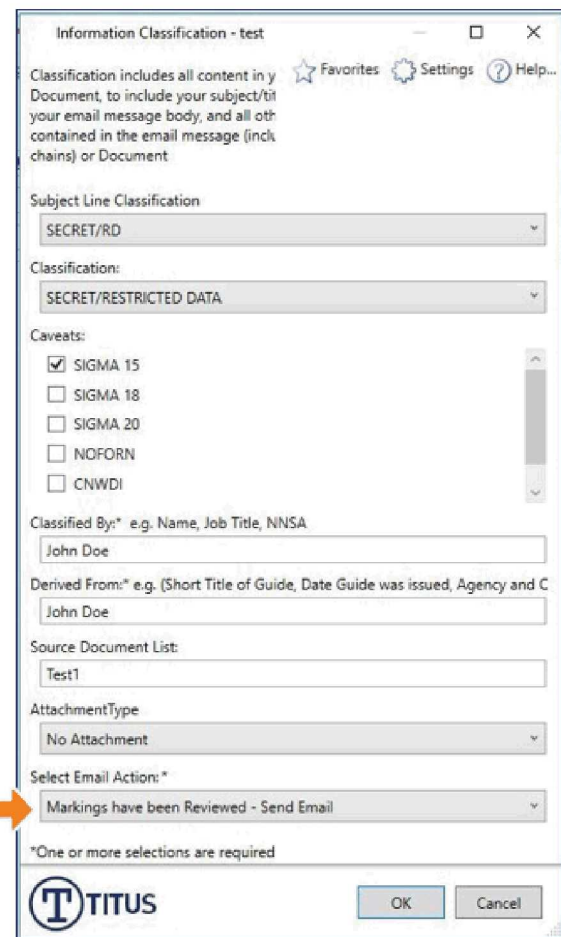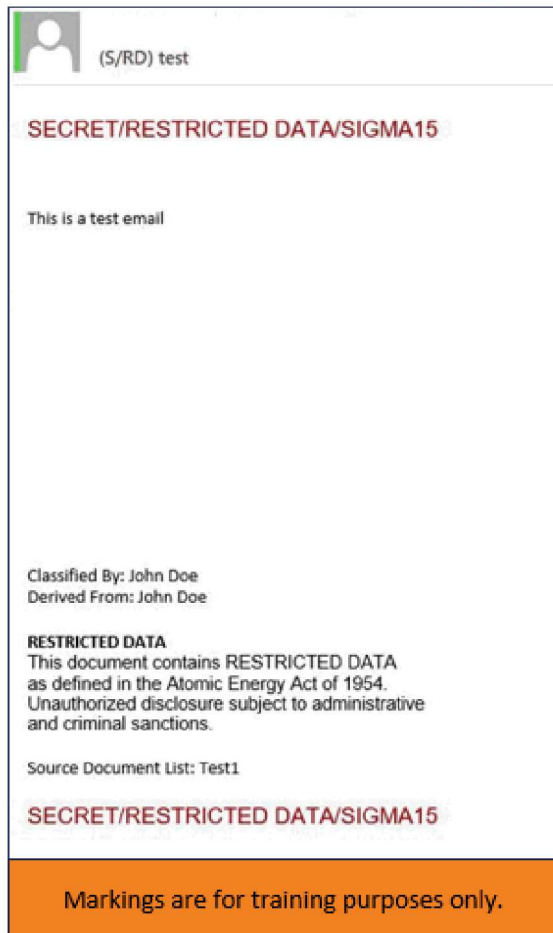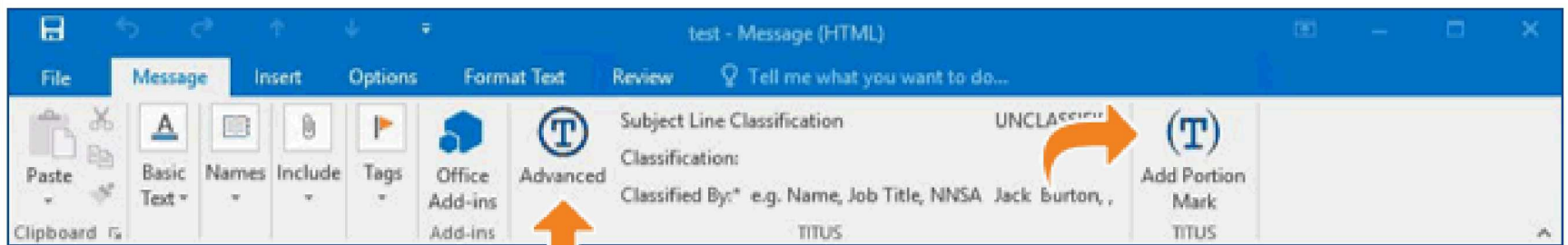
Presentation Agenda

- What is TITUS?

- Screen shots of TITUS product

- Why TITUS?

- Overview of the TITUS Project

- Additional Information about TITUS

- How are future updates to TITUS handled?

- Sandia Use Case
  - Early adopters
  - Sandia's TITUS Story
  - Sandia Setup and Support structure
  - Implementation
  - Metrics
  - Lessons Learned

- Questions?

- Contact Information

What is TITUS?

- TITUS is an email classification marking solution that standardizes the way we will mark/classify our emails by using a workflow interface that will allow us to quickly mark our email messages.
- It does this by automatically adding visual markings and handling instructions to emails. It applies dynamic headers, footers, watermarks, and other markings to raise user awareness about sensitivity of the content of the email.
- The selected solution includes TITUS Message Classification and Document Classification capabilities.

Screen Shots of TITUS

Markings are for training purposes only.

Why TITUS?

The Department of Energy (DOE) and National Nuclear Security Administration (NNSA) issued a memo dated July 26, 2017 to NNSA field offices and affected National Laboratories, informing them that TITUS was selected to meet policy requirements and its use will be required on all classified site systems

The memo states:

"NNSA has selected the TITUS classification suite as the enterprise solution for email and document markings on all Enterprise Secure Network (ESN) and NNSA Secret Network (NSN) connected systems."

"The NNSA OCIO has launched a project to design and deploy an enterprise-integrated TITUS solution."

**Department of Energy
National Nuclear Security Administration**
Washington, DC 20585

July 26, 2017

MEMORANDUM FOR   NNSA FIELD OFFICE MANAGERS AND AUTHORIZING OFFICIALS

FROM: SCOTT ENGELSON
DIRECTOR OF INFORMATION TECHNOLOGY AND
CYBERSECURITY OPERATIONS
NATIONAL NUCLEAR SECURITY ADMINISTRATION

SUBJECT: Enterprise standard for email and document marking

NNSA has selected the TITUS Classification Suite (TITUS) as the enterprise solution for email and document marking on all Enterprise Secure Network (ESN) and NNSA Secret Network (NSN) connected systems (SYSTEMS). The selected TITUS solution includes TITUS Message Classification and TITUS Document Classification capabilities. TITUS was selected by the NNSA Office of the Associate Administrator for Information Management and Chief Information Officer (NNSA OCIO; NA-IM) as the chosen solution to meet policy requirements and its use in an enterprise-integrated fashion is henceforth required on all site SYSTEMS. Any usage and licensing of the TITUS product beyond these SYSTEMS is outside the authority of this memo and at the discretion of individual sites.

TITUS Deployment Project Overview

- The TITUS email marking solution deployment is an NNSA OCIO/NA-IM managed project.
- The NNSA PMO, (Project Management Office) is managing this enterprise-wide rollout.
- Mark Holtzclaw, (from the PMO) is the Project Manager assigned to ensure TITUS is deployed to all ESN and NSN connected sites.
- **<u>Deployment Schedule:</u>**
  - Deployment packages will be available to all ESN sites in the early June timeframe.
  - Each site is responsible for the configuration and installation of the TITUS solution.

Additional information

- A centralized solution has been implemented so that each sites configuration file pulls from a centralized managed configuration file.

- Licensing will be also be managed from this centralized solution, so any site that already has TITUS implemented will no longer need to maintain their licensing.

- Each site will be responsible for providing any additional training not covered within the "TITUS User's Guide" provided with the deployment package.

Future Updates (How TITUS handles changes)

NA-746 (Classification & Controlled Information Division) will be managing all M&O activities and will maintain the master TITUS configuration file. All sites will automatically receive updates from the centralized server.

Additional support options include:

NNSA Mission Service Desk
missionservicedesk@nnsa.doe.gov / (505) 845-6900

TITUS support
support@titus.com / (866) 530-5111

Use case

Let's talk about email for a moment.

Email is a **business record** and is subject to litigation. Intel Paid AMD $1,200,000,000 for unfair business practices and emails were used in court.

Mismanagement of emails has financial consequences. Not being able to produce emails when obligated costs organizations between $1 million and $5 million.

"Last Mile" of compliance and governance – the last mile is the process of capturing, classifying, and storing important documents and emails.

When email is correctly classified (such as with PII) and stored, then emails and hard drives are protected, encrypted and backed up. So when **laptops are lost or stolen** (12,000 every week at US airports), correctly protected information doesn't generate those pesky "One Year Free Credit protection from Arbys".

Early adopters

Livermore in April 2017

Sandia in June 2017

Kansas City

Sandia's Titus story

Sandians on our classified network were marking emails based upon a marking guidelines document.

One group was using a custom, home grown Outlook tool

Use and support would not scale to the Sandia enterprise – We looked into that.

DOE order for email marking triggered our CMPC group to look for an automated solution.

Titus was selected on 8/1/2016.

Sandia's Titus story

Reviews were performed

   eSCRM – Link

    SAM - System for Award Management

     Titus was already in system

    CNARS – Classified Network Application Request System

Sandia purchased the Titus Classification Suite of tools – including Titus documents

   We launched Titus on our SCN in March of 2017

   We launched Titus on our SPN in June of 2017

Sandia will be installing Titus on our SRN network in 2018

Sandia's Setup

Low-side

    Database for admin console options

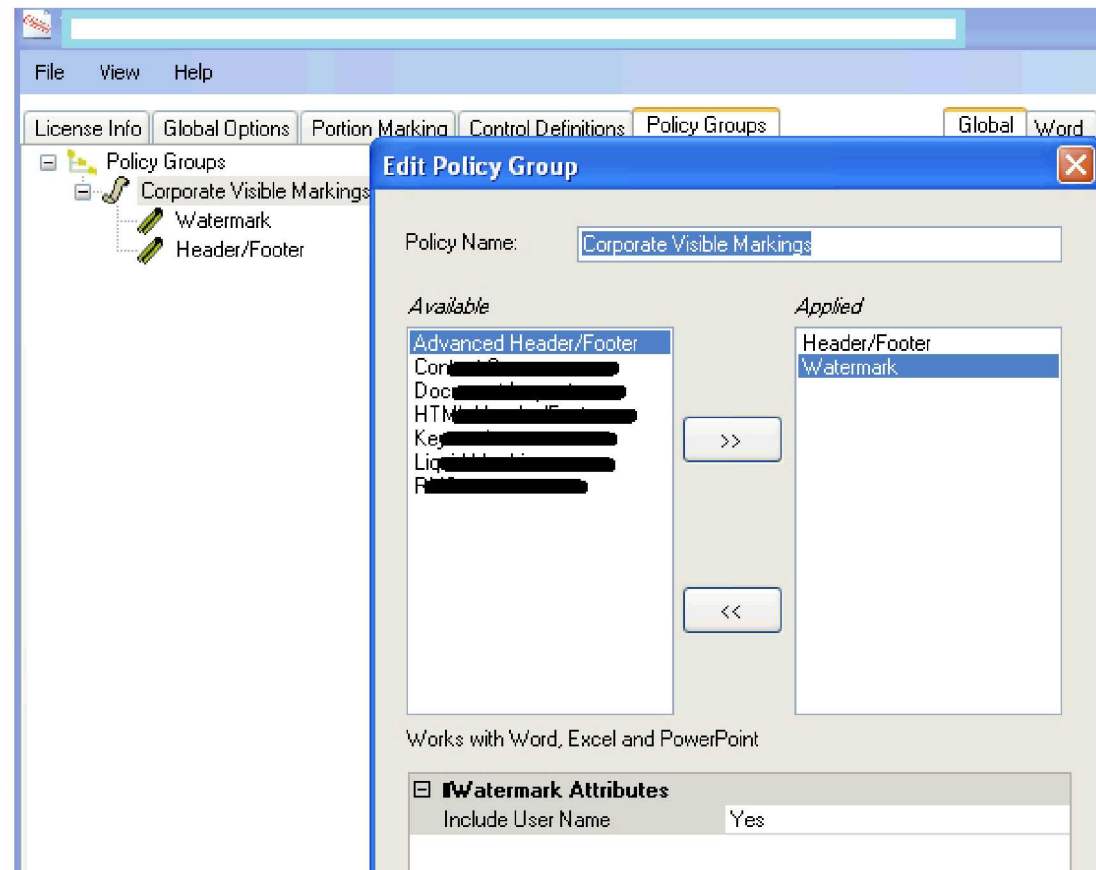   VM with Admin console for making changes to the config

    Dev environment (VM)

    QA environment (VM)

High side

    Prod environment

    Reporting (Splunk)

Sandia's Titus Support Structure

3CSI — Classified Computing Continual Service Improvement

3CSI program at Sandia facilitates bi-directional conversations that benefit the entire classified computing community, thereby producing a united front on the SCN, SPN, ESN and 3CSI activities

CCHD (Corporate Computing Help Desk)

      Sandia's central point for desktop computing and IT-related support

Red Rovers – Sandia's Classified remote desktop and deskside support staff

CMPC – Classified Matter Protection Control

Titus customization and support

Sandia's Implementation Project 1

Phase 1 – the SCN

4.5 months – not including Eval and purchasing

Team size 18

Five Sandia sites

Over 4000 users

	ⓘ	Task Mode	Task Name	Duration	Start	Finish	Prede	% Comp
7	✓		⊟ **Install and Configure**	**55 days**	**Tue 11/1/16**	**Mon 1/16/17**		**100%**
8	✓		⊞ **Admin Console**	**54 days**	**Tue 11/1/16**	**Fri 1/13/17**		**100%**
13	✓📓		⊞ **VDI Install**	**1 day**	**Tue 12/20/16**	**Wed 12/21/16**	10	**100%**
15	✓📓	📌	SQL Database Install	2 days	Mon 11/28/16	Wed 11/30/16	8	100%
16	✓📓	📌	Configure parts to talk to each other	1 day	Tue 12/6/16	Tue 12/6/16	15	100%
17	✓		Roll out of Templates	1 day	Mon 1/16/17	Mon 1/16/17		100%
18	✓	📌	Communication Plan	3 wks	Thu 1/5/17	Wed 1/25/17		100%
19	✓	📌	OLA with CCHD - Christina	1 wk	Mon 1/16/17	Fri 1/20/17		100%
20	✓	📌	⊟ **Training**	**17 days**	**Mon 1/23/17**	**Tue 2/14/17**		**100%**
21	✓	📌	Sysadmin (ongoing) Training	2 wks	Wed 1/11/17	Tue 1/24/17	6	100%
22	✓		User Training	8 days	Mon 1/23/17	Wed 2/1/17		100%
23	✓	📌	CSU training	1 wk	Mon 1/16/17	Fri 1/20/17	10	100%
24	✓	📌	Red Rover Training	1 day	Mon 1/23/17	Mon 1/23/17		100%
25	✓	📌	Documentation	1 day	Tue 1/10/17	Tue 1/10/17		100%
26	✓📓	📌	CA integration	0 wks	Wed 1/4/17	Tue 1/17/17	17	100%
27	✓		⊟ **Testing**	**18 days**	**Wed 1/11/17**	**Fri 2/3/17**		**100%**
28	✓	📌	Alpha Testing	2 days	Wed 1/11/17	Thu 1/12/17		100%
29	✓📓	📌	Pilot Testing - VDI pool	2 wks	Mon 1/23/17	Fri 2/3/17	17	100%
30	✓📓	📌	SCCM Deployment Testing	1 day	Mon 1/16/17	Mon 1/16/17	17	100%
31	✓📓	📌	User Testing (Beta testing)	7 days	Mon 1/23/17	Tue 1/31/17	17	100%
32	✓		⊟ Gamma testing on SCN	1 day	Wed 2/1/17	Wed 2/1/17		100%
33	✓	📌	⊞ **Entrust Testing**	**1 day**	**Wed 2/1/17**	**Wed 2/1/17**	31	**100%**
35	✓		⊞ **Reporting**	**1 day**	**Thu 1/12/17**	**Thu 1/12/17**		**100%**
37	✓	📌	⊞ **Approvals**	**1 day**	**Thu 12/15/16**	**Thu 12/15/16**		**100%**
43	✓		⊟ **Deployment**	**283 days**	**Mon 2/13/17**	**Wed 3/14/18**		**100%**
44	✓	📌	NM Deployment	2.2 wks	Tue 2/28/17	Tue 3/14/17		100%
45	✓	📌	⊟ **CA Deployment**	**56.6 wks**	**Mon 2/13/17**	**Wed 3/14/18**		**100%**
46	✓	📌	On-site Brown Bag Training	5 days	Mon 2/13/17	Fri 2/17/17		100%
47	✓	📌	CA Deployment	2.2 wks	Tue 2/28/17	Tue 3/14/17	46	100%
48	✓	📌	DC Deployment	2.2 wks	Tue 2/28/17	Tue 3/14/17		100%
49	✓	📌	Carlsbad Deployment	2.2 wks	Tue 2/28/17	Tue 3/14/17		100%
50	✓	📌	MN Deployment	2.2 wks	Tue 2/28/17	Tue 3/14/17		100%
51	✓	📌	Long Term maintenance and support decisions	10 days	Thu 8/11/16	Wed 8/24/16	11	100%

Sandia's Implementation Project 2

Phase 2 - the SPN - (Sandia Partner Network)

3 months, but less work

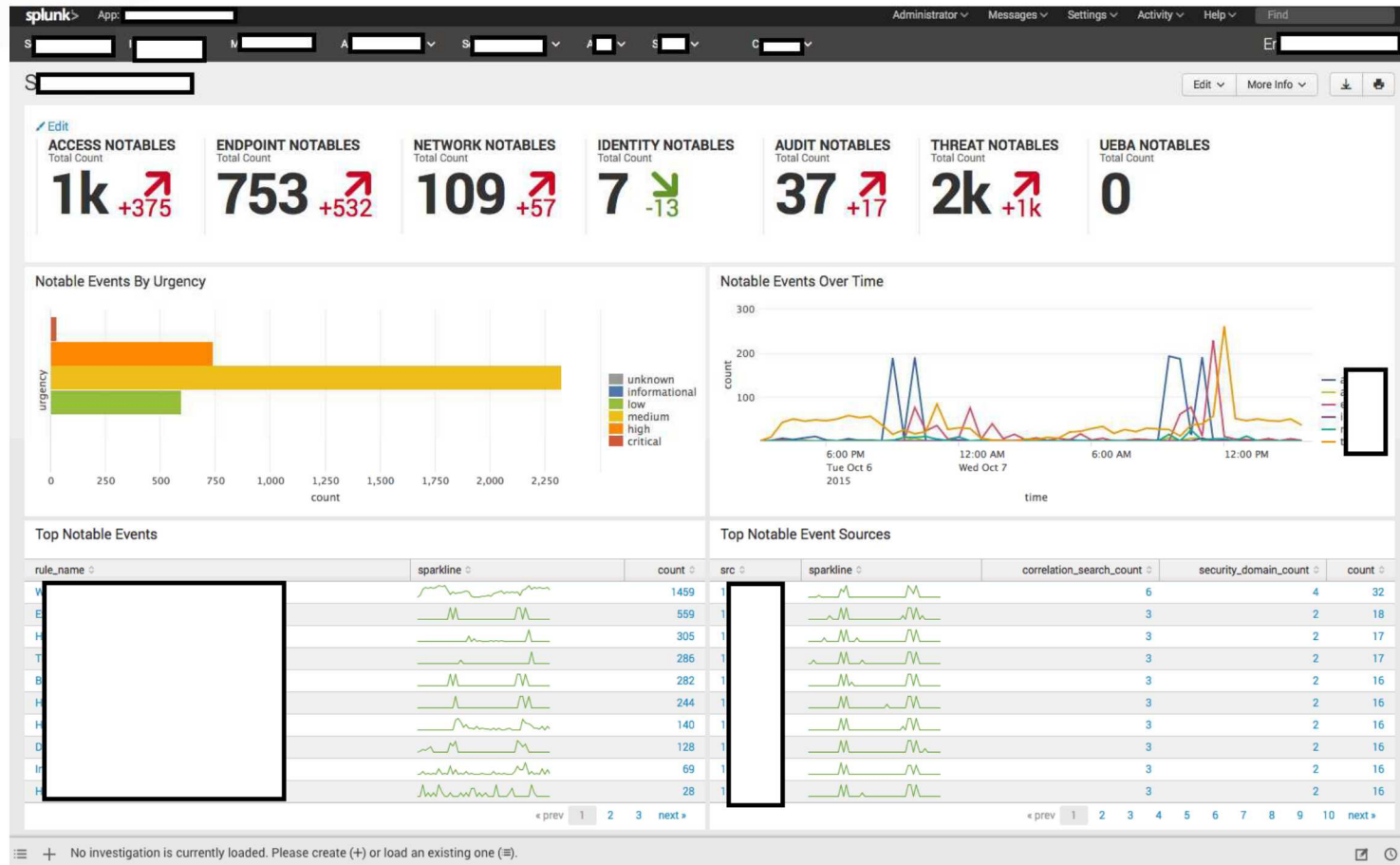Purposely stayed at version 4.6 so as to not get ahead of the NNSA install.

Rinse and repeat of Phase 1 – used the same team

		Task Mode	Task Name	Duration	Start	Finish	Pr	% Complet
1	✓	📌	Config file adjustment	1 day	Tue 3/28/17	Tue 3/28/17		100%
2	✓	📌	STIGS compliance	1 day	Tue 3/28/17	Tue 3/28/17		100%
3	✓	📌	Support	1 day	Tue 3/28/17	Tue 3/28/17		100%
4	✓	📌	App owner decision and Roles	1 day	Tue 3/28/17	Tue 3/28/17		100%
5	✓		□ **Reporting**	**251 days**	**Wed 3/29/17**	**Wed 3/14/18**		**100%**
6	✓	📌	Splunk Client Install	221 days	Wed 5/10/17	Wed 3/14/18		100%
7	✓	📌	Install testing	251 days	Wed 3/29/17	Wed 3/14/18	6	100%
8	✓	📌	Report generation testing	216 days	Wed 5/17/17	Wed 3/14/18	7	100%
9	✓	📌	eCAB for Splunk	231 days	Wed 3/29/17	Wed 2/14/18		100%
10	✓	📌	Communication Plan	7 days	Wed 6/14/17	Thu 6/22/17		100%
11	✓	📌	Testing - Alpha, Beta	10 days	Wed 6/7/17	Tue 6/20/17		100%
12	✓	📌	eCAB	1 day	Thu 6/8/17	Thu 6/8/17	11	100%
13	✓	📌	Deployment	1 day	Wed 6/21/17	Wed 6/21/17	12	100%
14	✓	📌	NNSA syncronization	1 day	Tue 3/28/17	Tue 3/28/17		100%
15	✓	📌	Lessons Learned and closeout	1 day	Wed 6/28/17	Wed 6/28/17		100%

Sandia's Metrics

For the Implementation:
85% saturation in 7 days

For the reporting of yearly metrics:
Sandia choose to utilize the Splunk option for reporting

Spunk sample screenshot – not related to Titus

Sandia's lessons learned 1

Things that went well:

Engaged Sandia support teams early

Several had their own processes to onboard support of an application

Utilized the 3CSI communication methods

Previously established and trusted team, methods, and infrastructure

Internal Sharepoint Website – both low and high side networks

Trusted email communication channel already in use.

Brown Bag informational sessions – CA and NM

Testing

Utilized users from different sites, managers, and high use groups

This really helped to have local champions – and their feedback

Utilized CMPC users

To verify CMPC rules were implemented correctly

Engagement with Titus expert

Our Titus expert came onsite and helped translate our marking rules into the config file and helped with server setup along with reporting guidance.

Sandia's lessons learned 2

Things that could have gone better:

App Owner not identified early

Important for early training and setup of configuration file

Important for understanding CMPC rules and the interaction with the config file - and ownership of the config file.

Deployment issues

Installer issue - Titus deployed early on a few systems

Testing

Test scripts could have been more like real life use

Don't use humor.

Contact Information:

- NNSA TITUS Project Manager (Mark Holtzclaw)
  - Mark.Holtzclaw@nnsa.doe.gov / (505) 697-2065

- NNSA Mission Service Desk
  - missionservicedesk@nnsa.doe.gov / (505) 845-6900

- Sandia National Laboratories Project Manager (Mark Timms)
  - lmtimms@snl.gov / (505) 845-3568

- TITUS support
  - support@titus.com / (866) 530-5111