CYBER DASHBOARD PILOT

COL Mike J. Jones, SAIS-CB
michael.jones6@us.army.mil, DSN 703.839.3648

Cyber Dashboard Pilot Overview

Pilot Purpose:

Reduction in overall cyber risks due to increase level of compliance with IA policies and network security standards.

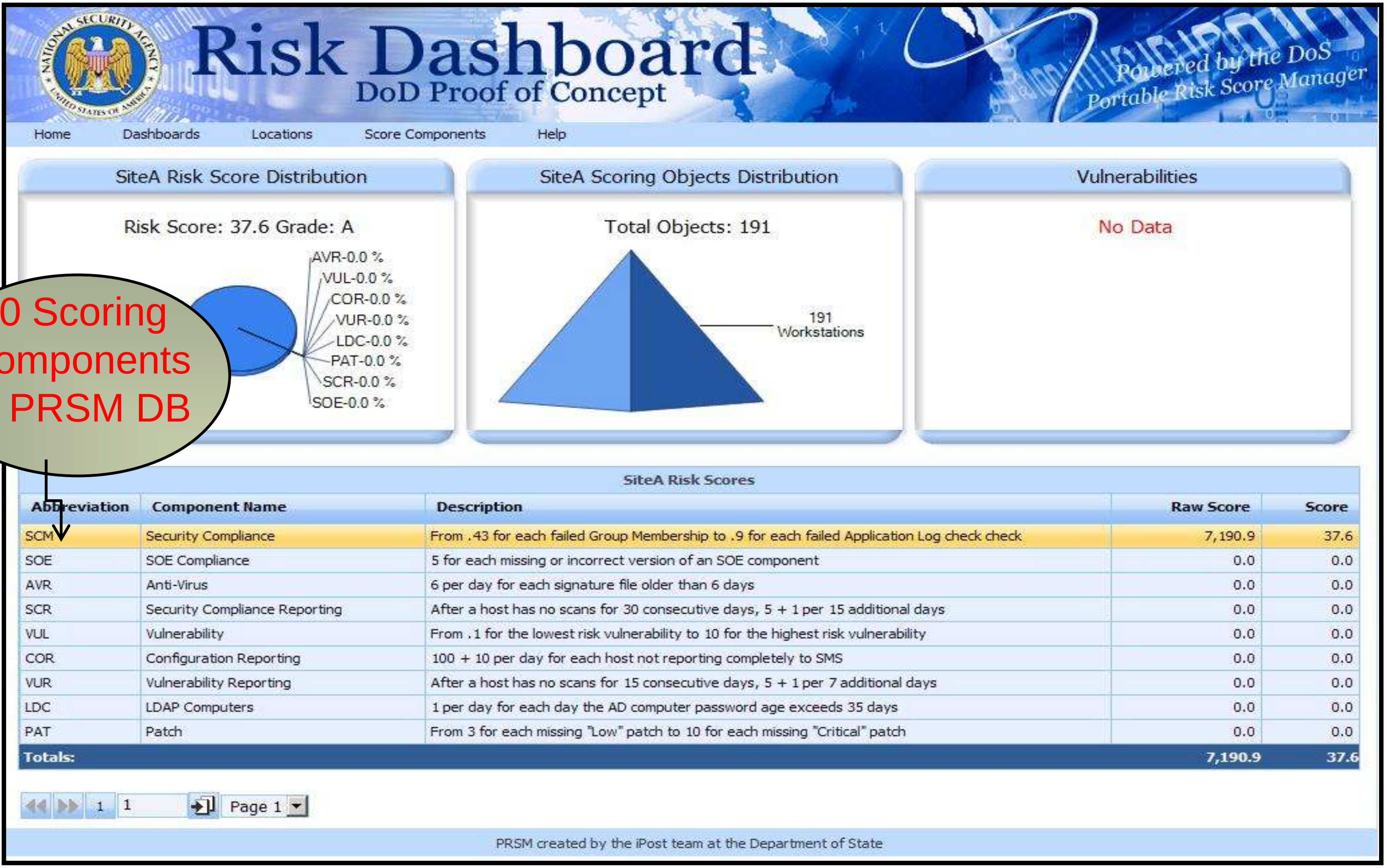
Pilot Mission:

Improve the Army's Information Assurance (IA) and Cyber security posture.

Concept of Operations:

Establish a scorecard which reports on an asset's level of compliance to given standards using the Dept. of States Portable Risk Score Manager (PRSM) and leveraging System Center Configuration Manager (SCCM), CA Unicenter, and Host Based Security System (HBSS) deployed technologies.

Cyber Dashboard Risk View



SiteA Risk Score Distribution

Risk Score: 37.6 Grade: A

SiteA Scoring Objects Distribution

Total Objects: 191

Vulnerabilities

No Data

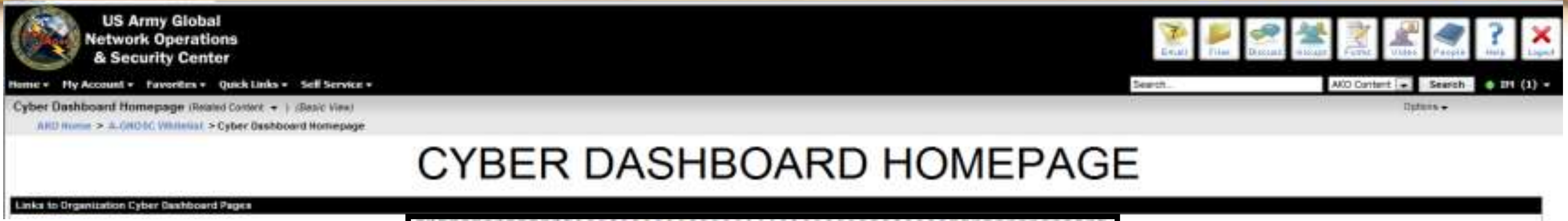
10 Scoring Components In PRSM DB

SiteA Risk Scores

Abbreviation	Component Name	Description	Raw Score	Score
SCM	Security Compliance	From .43 for each failed Group Membership to .9 for each failed Application Log check check	7,190.9	37.6
SOE	SOE Compliance	5 for each missing or incorrect version of an SOE component	0.0	0.0
AVR	Anti-Virus	6 per day for each signature file older than 6 days	0.0	0.0
SCR	Security Compliance Reporting	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days	0.0	0.0
VUL	Vulnerability	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability	0.0	0.0
COR	Configuration Reporting	100 + 10 per day for each host not reporting completely to SMS	0.0	0.0
VUR	Vulnerability Reporting	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days	0.0	0.0
LDC	LDAP Computers	1 per day for each day the AD computer password age exceeds 35 days	0.0	0.0
PAT	Patch	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch	0.0	0.0
Totals:			7,190.9	37.6

PRSM created by the iPost team at the Department of State

Cyber Dashboard DA View



US Army Global Network Operations & Security Center

Home ▾ My Account ▾ Favorites ▾ Quick Links ▾ Self Service ▾

Search... AKO Content ▾ Search

Cyber Dashboard Homepage (Related Content ▾ | (Basic View)

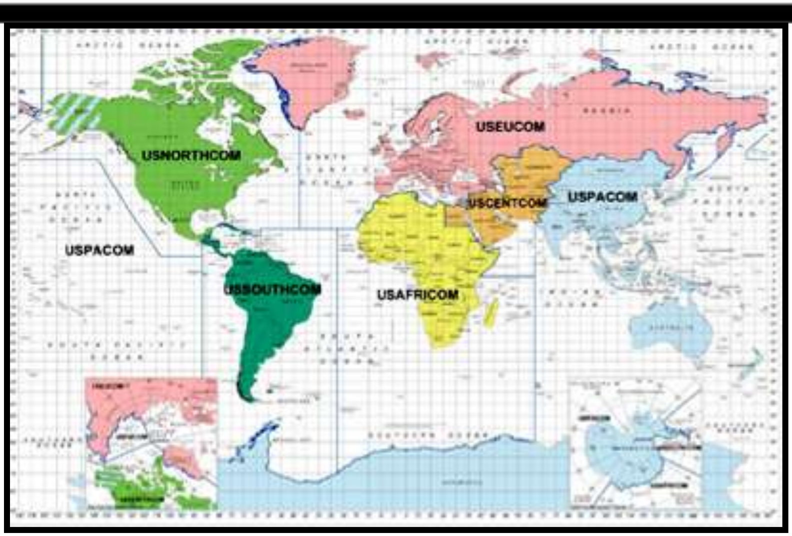
Options ▾

AKO Home > A-GNOSC Whitelist > Cyber Dashboard Homepage

CYBER DASHBOARD HOMEPAGE

Links to Organization Cyber Dashboard Pages

AMC
ARNG
ASA(ALT)
ATEC
EUSA
FMWRC
FORSCOM
IMCOM
INSCOM
MDW
MEDCOM
NETCOM/9th SC(A)
OAA HQDA
TRADOC
USAASC
USACE
USACIDC
USARC
USARCENT
USAREUR
USARNORTH
USARPAC
USARSO
USASMDC/ARSTRAT
USASOC
USJFCOM
USMA
SDDC



NIPR
Risk Level Grade: TBD
Hosts: TBD

SIPR
Risk Level Grade: TBD
Hosts: TBD

Honorable John M. McHugh
Secretary of the U.S. Army

GEN George W. Casey Jr.
Chief of Staff of the U.S. Army

LTG Jeffrey A. Sorenson
Chief Information Officer/G-6

Cyber Dashboard Commander View

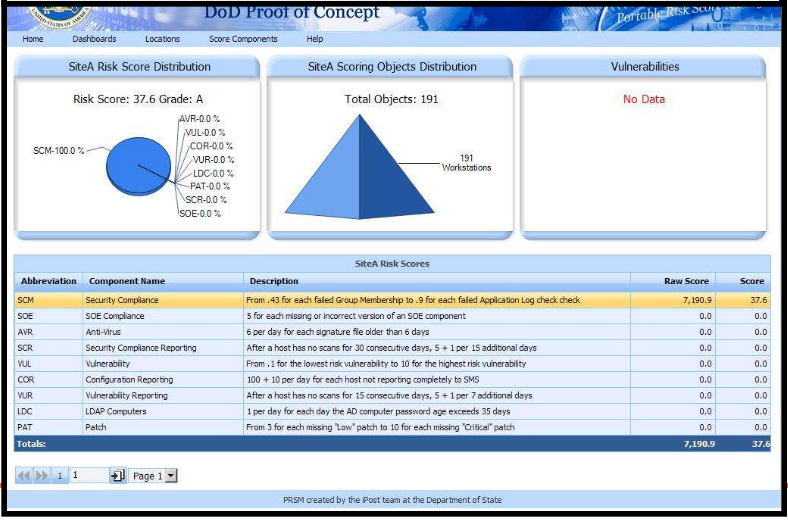
9th SC (A)/NETCOM CYBER SCORECARD

a. Network Service Providers.
MSC A
MSC B
MSC C

b. System Owners
MSC A
MSC B
MSC C

c. Users Only
MSC A
MSC B
MSC C

USEUCOM
USNORTHCOM
USCENTCOM
USPACOM
USPACOM
USSOUTHCOM
USAFRICOM



SiteA Risk Score Distribution

Risk Score: 37.6 Grade: A

SiteA Scoring Objects Distribution

Total Objects: 191

Vulnerabilities

No Data

SiteA Risk Scores

Abbreviation	Component Name	Description	Raw Score	Score
SCM	Security Compliance	From .43 for each failed Group Membership to .9 for each failed Application Log check check	7,190.9	37.6
SOE	SOE Compliance	5 for each missing or incorrect version of an SOE component	0.0	0.0
AVR	Anti-Virus	6 per day for each signature file older than 6 days	0.0	0.0
SCR	Security Compliance Reporting	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days	0.0	0.0
VUL	Vulnerability	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability	0.0	0.0
COR	Configuration Reporting	100 + 10 per day for each host not reporting completely to SMS	0.0	0.0
VUR	Vulnerability Reporting	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days	0.0	0.0
LDC	LDAP Computers	1 per day for each day the AD computer password age exceeds 35 days	0.0	0.0
PAT	Patch	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch	0.0	0.0
Totals:			**7,190.9**	**37.6**

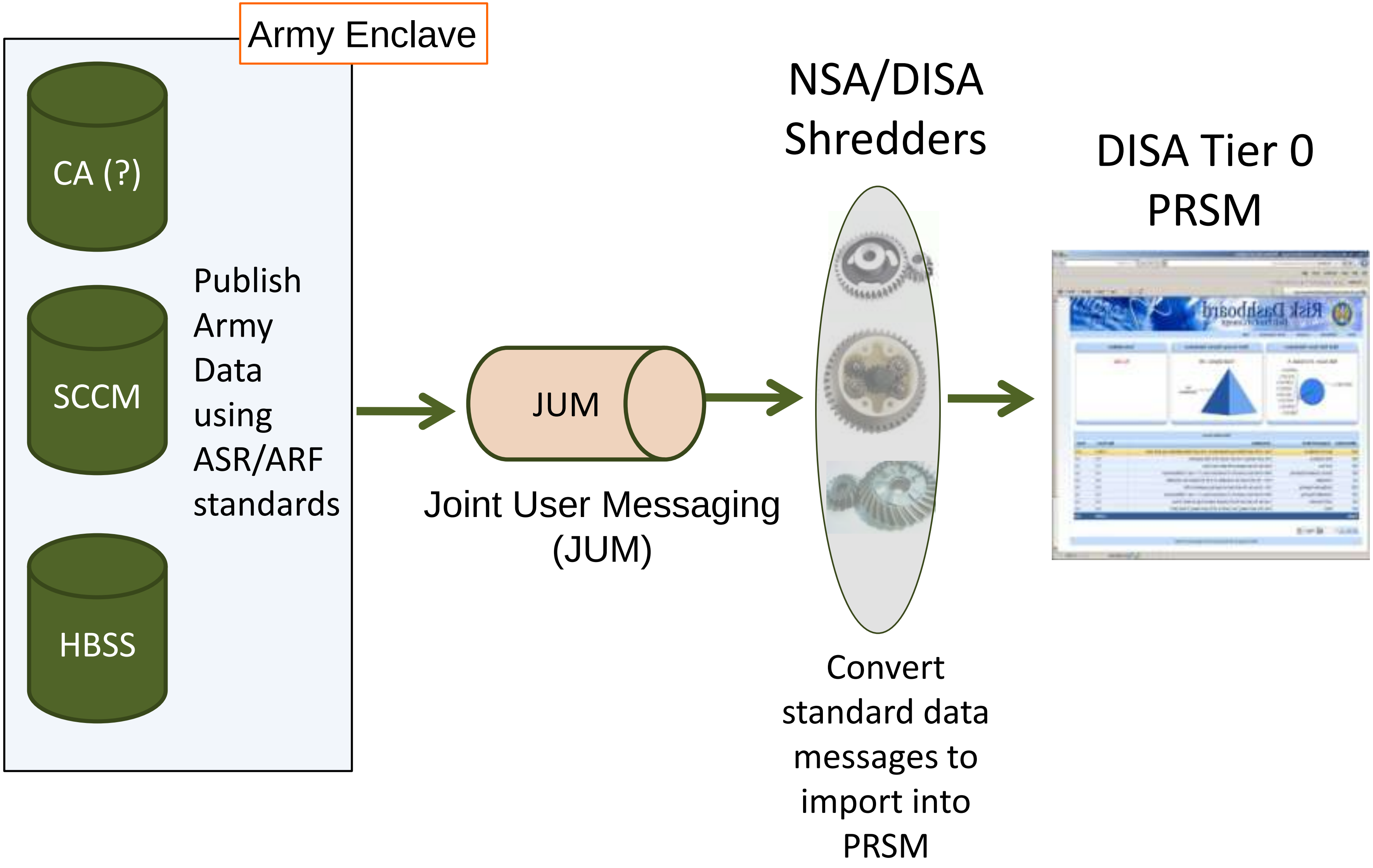
PRSM created by the iPost team at the Department of State

BG Napper
9thSC(A)/NETCOM

NIPR
Risk Level Grade: TBD
Rank in Enterprise: TBD
Hosts: TBD

SIPR
Risk Level Grade: TBD
Rank in Enterprise: TBD
Hosts: TBD

Continuous Monitoring Architecture



Army Enclave

CA (?)

SCCM

HBSS

Publish Army Data using ASR/ARF standards

JUM

Joint User Messaging (JUM)

NSA/DISA Shredders

Convert standard data messages to import into PRSM

DISA Tier 0 PRSM

Continuous Monitoring (CM)

Next Steps:

1. Publish Lessons Learned from Pilot 1QFY11
2. Publish CM Policy/Guidance 2QFY11
3. Publish CM Requirements 2QFY11
4. Publish CM Implementation Plan 3QFY11
5. Execute CM Implementation Plan 4QFY11

Wrap-Up

Questions?

Pilot Updates on CIO/G-6 SharePoint:

https://intranet.hqda.ds.army.mil/ciog6/cyber/projmgmt

Pilot Updates on Intelink:

https://www.intelink.gov/sites/gig-ia/ECMC/armycdpilot/default.aspx

For More Information on the Cyber Dashboard Contact:

COL Mike Jones, michael.jones6@us.army.mil , 703.839.3648