SPIN 15 VPN Story

VPN has two thrusts, one has high mission impacts and the other has high performance and functionality impacts for Program B.

Mission impact – Start generating SIGINT from VPNs at SMK.

SMK is a VPN rich environment with targets of high value. Mission impact is high. Consumers of the SIGINT reporting based on sources from SMK are at high levels of government. NSA leadership has tasked CES to deploy decryption capabilities to SMK. Security concerns have been addressed. SPFs have been signed to deploy TS//SI equities to the S//SI site. VPN transformation tests have passed and capabilities ready for deployment to the T-16 development server at SMK. To achieve a successful deployment to SMK on the T-16s (first) and LPTs, the following are high level steps:

Task	Owner	Date
Load Spin 13 on T-16 DEV (first) and then T-16 LIVE system	Turmoil	March
Configure Blade 14 for PIQ Services Spin 13.	CES	March
Configure AMF/IslandHideaway for PIQ blade and VAO messaging traffic	AMF	March
Add IP tasking to Keycard for VPNs of interest	CES	March
Evaluate decrypted data in Xkeyscore for Strong Selectors	CES	March/April
Update Keycard with Strong Selectors	CES	March/April
Verify decrypted data which hits on a strong selector is forwarded from Turmoil to Pressurewave	CES	April
Verify analysts can retrieve the data from Pressurewave for reporting	CES	April
Identify Dell for PIQ Blade at SMK for LPT DEV system	CES	April
Load Spin (13/14 ?) on LPT DEV (first) and then the LPT LIVE Systems	Turmoil	May
Configure Dell for PIQ Services Spin 13.	CES	May

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Configure AMF/IslandHideaway for PIQ blade and VAO messaging traffic	AMF	May
Add IP tasking to Keycard for VPNs of interest	CES	May
Evaluate decrypted data in Xkeyscore for Strong Selectors	CES	May/June
Update Keycard with Strong Selectors	CES	May/June
Verify decrypted data which hits on a strong selector is forwarded from Turmoil to Pressurewave	CES	June
Verify analysts can retrieve the data from Pressurewave for reporting	CES	June

Note: MDC upgrade and Site Store deployment at SMK will impact the VPN decryption deployment. March 16-31 is the schedule for the upgrade and site store deployment. VPN decryption deployment may slip due to availability.

Risk Reduction Activity for Program B

Program B Capabilities Document has provided Key Performance Paramerters (KPPs) for VPN. In order to achieve the KPP identified for Sep 30, 2009, a risk reduction activity has been initiated. This activity will gather performance benchmarks early in SPIN 15 on the current architecture running on two 2.5G platforms, the T-16 Heavy and the Dell LPT. Information from the performance benchmarks will indicate the level of redesign (if any) needed to meet the KPPs. The following are the performance requirements in Program B.

1.	NCC CA Service Requests (Decrypt) per hour (aggregate for all VPN exploitation-enabled systems).			
	Q4 FY09 (Risk Reduction)	1,000		
	Q4 FY10	10,000		
	Q4 FY11	100,000		
2.	NCC front end systems shall fully process (i.e. decrypt and re-inject) at least 20% of CA service requests (~20% Reinject Rate?)			
3.	For tasked IP addresses, NCC front end systems shall identify relevant IPSec sessions and generate attack requests (Rates?)			
4.	NCC front end systems shall buffer VPN data for up to 15 minutes (900 seconds) while waiting for response from Attack Orchestrater (AO)			
5.	After successful key recovery and decryption PIQ services shall re-inject decrypted VPN for Stage1 & Stage2 processing			
6.	Aggregate VPN buffering and processing rate per TML system (**Assumptions – LPT? T16? U64?**)			
	Q4 FY09 (Risk	4 VPN	25 Concurrent VPN	100 Mbps Aggregate VPN Data / System

Reduction)	Systems	Flows / System	
Q4 FY10	10 VPN Systems	100 Concurrent VPN Flows / System	100 Mbps Aggregate VPN Data / System
Q4 FY11	100 VPN Systems	100 Concurrent VPN Flows / System	500 Mbps Aggregate VPN Data / System

7. Desired SSL Exploitation - Aggregate TURMOILs shall exploit all sessions associated with a given cryptovariable at the rates:

Q4 FY09 (Risk Reduction)	10,000 Sessions / Day
Q4 FY10	100,000 Sessions / Day
Q4 FY11	1,000,000 Sessions / Day
Q4 FY12	10,000,000 Sessions / Day

8. Desired Password Recovery - Aggregate TURMOILs shall detect the presence of at least 100 password based encryption applications at the rates:

Q4 FY09 (Risk Reduction)	500 Sessions / Month
Q4 FY10	2,000 Sessions / Month
Q4 FY11	8,000 Sessions / Month
Q4 FY12	20,000 Sessions / Month

A schedule has been proposed to gather the performance benchmarks on current turmoil 2.5G systems (T-16 and LPT).

Benchmark functionality and performance testing on TBAR 2.5G T-16		
Task	Owner	Date
Configure T-16 with SPIN 13. Configure Keycard	Turmoil	April 1-3
Configure Blade 14 in T-16 with PIQ services	CES	April 1-3
Configure ITx/IH for PIQ blade and VAO messaging traffic	AMF	April 1-3
Run PIQ to VAO interface test	CES	April 6
Provide data set that can be looped to meet performance requirements. Data set is characterized for outcome. Data needs to be loaded in streamer (?)	CES and Turmoil	April 6
Load Keycard with IPs and Strong Selectors	CES	April 6
Run test	CES and Turmoil	April 7-8
Identify issues	CES and Turmoil	April 9-10

Fix issues	CES and Turmoil	April 9-10
Rerun test	CES and Turmoil	April 9-10
Document Benchmarks	CES and Turmoil	April 13-15

April 16 will be a review date of the performance benchmarks gathered on a 2.5G T-16 Heavy system. This information will guide decisions to pursue architectural and design planning and implementation to meet the Sep 30, 2009 KPPs.

Benchmark functionality and performance testing on 2.5G LPT (T-16)		
Task	Owner	Date
Configure LPT with SPIN 14. Configure Keycard	Turmoil	April 30
Configure Dell with PIQ services	CES	April 30
Configure ITx/IH for PIQ blade and VAO messaging traffic	AMF	April 30
Run PIQ to VAO interface test	CES	April 30
Provide data set that can be looped to meet performance requirements. Data set is characterized for outcome. Data needs to be loaded in streamer (?)	CES and Turmoil	April 31
Load Keycard with IPs and Strong Selectors	CES	April 31
Run test	CES and Turmoil	May 1
Identify issues	CES and Turmoil	May 1
Fix issues	CES and Turmoil	May 4-5
Rerun test	CES and Turmoil	May 6
Document Benchmarks	CES and Turmoil	May 7

May 8 is the second review date of the performance benchmarks. This will include the benchmarks from the 2.5G LPT system. This information will guide decisions to pursue architectural/design planning and implementation to meet the Sep 30, 2009 KPPs.

Turmoil technical discussion can be hosted in parallel to the benchmark testing. The purpose of the discussions is to ??????.