NIPRNet/SIPRNet Cyber Security Architecture Review

21 April 2016

NSCSAR

NIPRNet/SIPRNet Cyber Security Architecture Review

NSA DoD CIO DISA

Pete Dinsmore
NSCSAR Chair

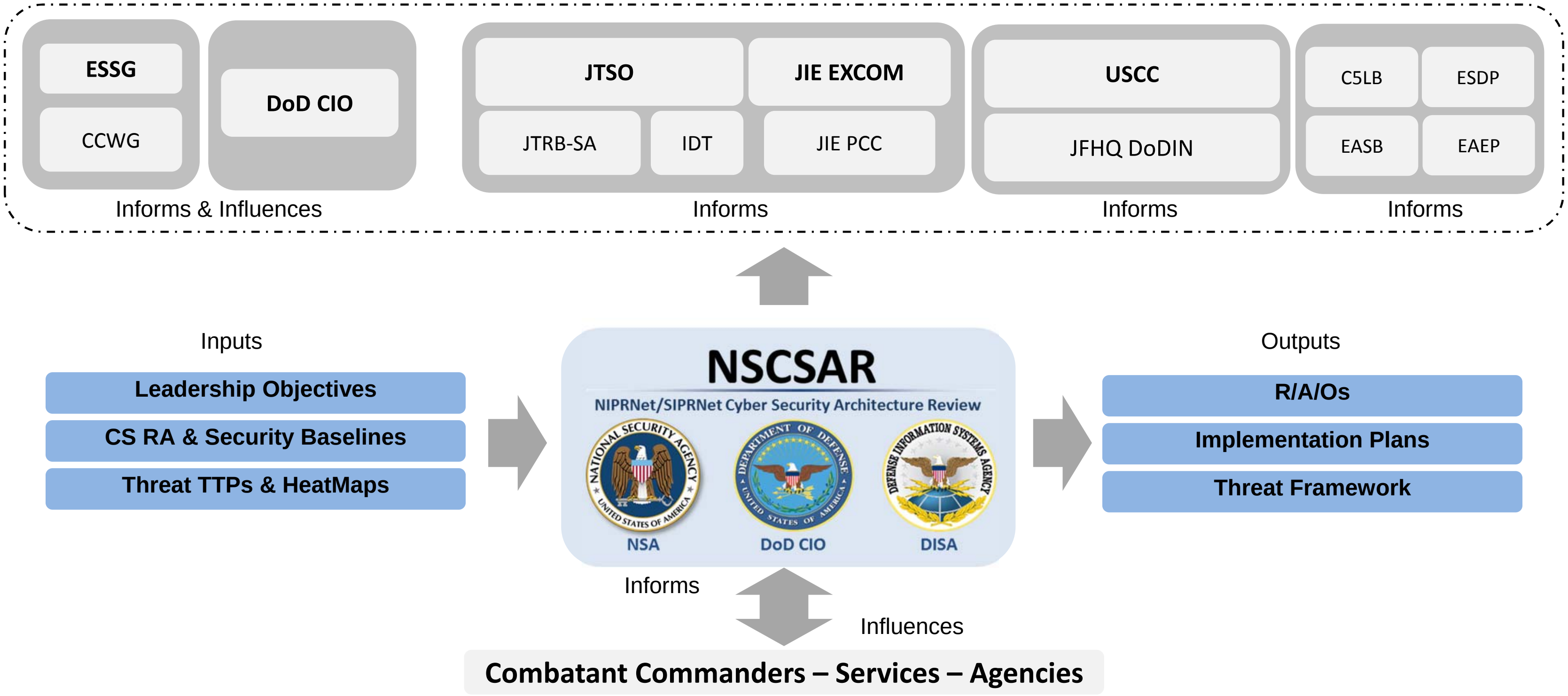
Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to Unite States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments.

NSCSAR Charter

- VISION
  - DOD has the insight and knowledge necessary to make prioritized capability decisions to enable dependable mission execution on the Unclassified and Secret Fabrics.
- PURPOSE
  - Evolve the cybersecurity architecture as necessary and create an implementation road map for the DODIN infrastructure based on an end-to-end holistic review of the security architecture and current implementations and plans. Create a solid rationale using the Cyber Kill Chain as a framework, informed by current classified and unclassified threat data.

NSCSAR Relationships



ESSG

CCWG

DoD CIO

Informs & Influences

JTSO

JIE EXCOM

JTRB-SA

IDT

JIE PCC

Informs

USCC

JFHQ DoDIN

Informs

C5LB

ESDP

EASB

EAEP

Informs

Inputs

- Leadership Objectives
- CS RA & Security Baselines
- Threat TTPs & HeatMaps

NSCSAR

NIPRNet/SIPRNet Cyber Security Architecture Review

NSA

DoD CIO

DISA

Outputs

- R/A/Os
- Implementation Plans
- Threat Framework

Informs

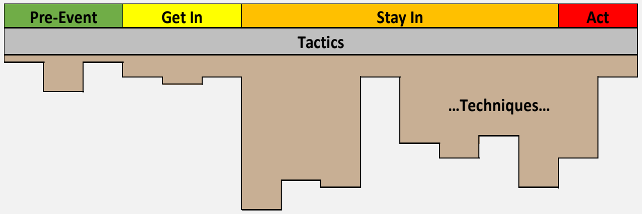
Influences

Combatant Commanders – Services – Agencies

Informs	-Information Inputs
Influences	-Information Inputs and Directly Affects Decision Making

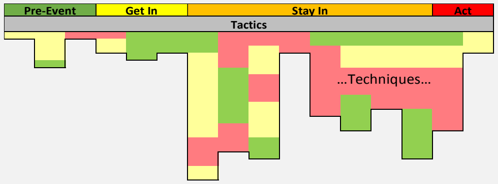
NSCSAR Concept

Threat Framework



Heat Maps – Intrusion Sets – Use Cases

R/A/Os



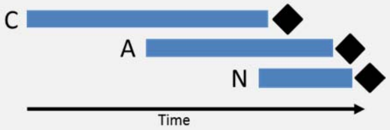
Capability Coverage Maps
Scenarios – Gaps – Redundancies

1 – Capability **C**
2 – Capability **A**
3 – Capability **N**
:

Priority Areas

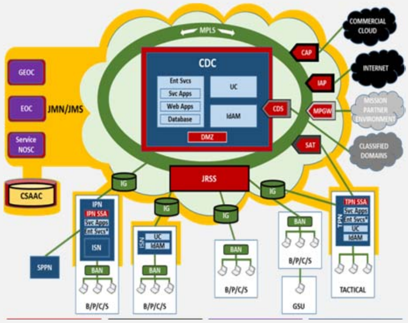
Sandboxed Browser
Trusted Host OS
Host-Based Firewall
Workstation or Laptop

Paradigm Shifts



Implementation Plans

Cyber Security Capabilities



-Perimeter

-Midpoint

-CC/S/As

-Endpoint

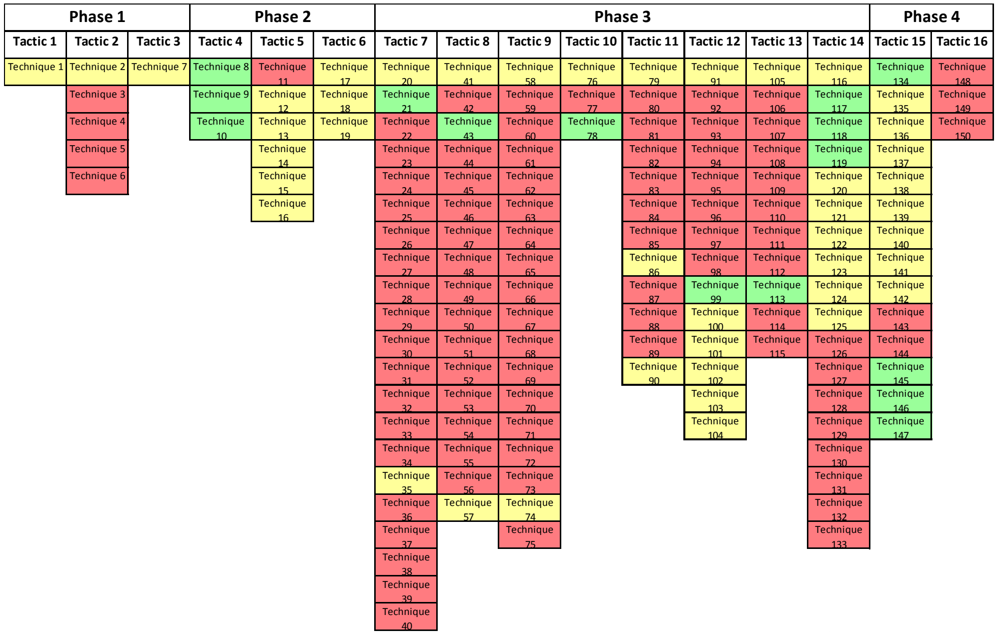
Capability Mitigation Scoring

	Pre-Event					
	Tactic					
	Technique			Technique		
Perimeter	Protect	Detect	Respond	Protect	Detect	Respond
Capabilities						
	🟩					
					🟩	
	🟥		🟥			
			🟨			
	🟨			🟥		
				🟥		
				🟥		

Significant – Moderate - Little

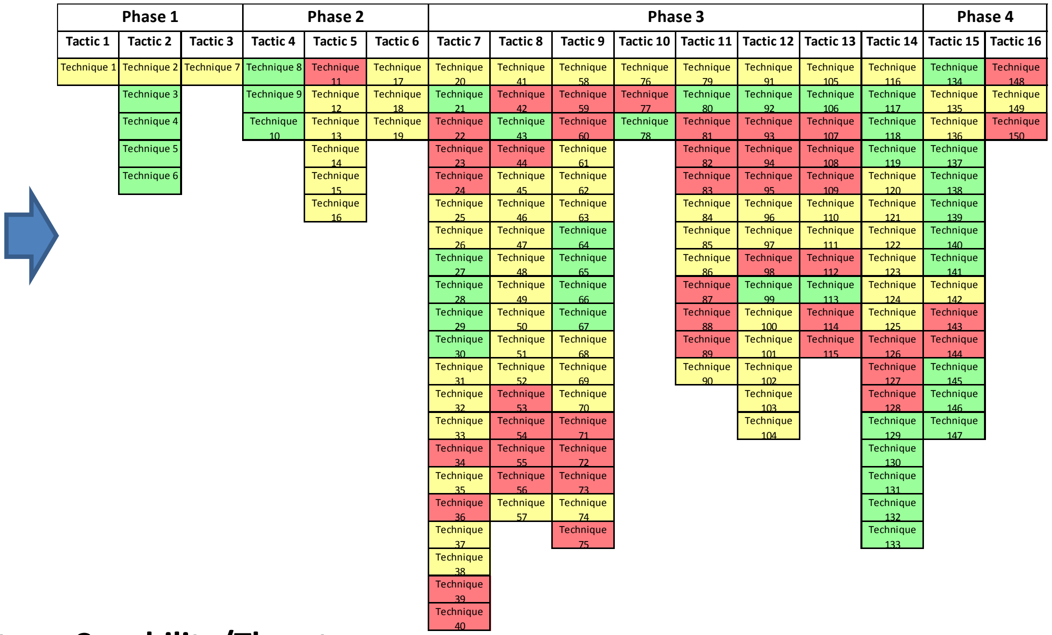
Threat Framework Example

'As-Is' DoDIN Security Capabilities (Example)



Phase 1			Phase 2			Phase 3								Phase 4	
Tactic 1	Tactic 2	Tactic 3	Tactic 4	Tactic 5	Tactic 6	Tactic 7	Tactic 8	Tactic 9	Tactic 10	Tactic 11	Tactic 12	Tactic 13	Tactic 14	Tactic 15	Tactic 16
Technique 1	Technique 2	Technique 7	Technique 8	Technique 11	Technique 17	Technique 20	Technique 41	Technique 58	Technique 76	Technique 79	Technique 91	Technique 105	Technique 116	Technique 134	Technique 148
	Technique 3		Technique 9	Technique 12	Technique 18	Technique 21	Technique 42	Technique 59	Technique 77	Technique 80	Technique 92	Technique 106	Technique 117	Technique 135	Technique 149
	Technique 4		Technique 10	Technique 13	Technique 19	Technique 22	Technique 43	Technique 60	Technique 78	Technique 81	Technique 93	Technique 107	Technique 118	Technique 136	Technique 150
	Technique 5			Technique 14		Technique 23	Technique 44	Technique 61		Technique 82	Technique 94	Technique 108	Technique 119	Technique 137	
	Technique 6			Technique 15		Technique 24	Technique 45	Technique 62		Technique 83	Technique 95	Technique 109	Technique 120	Technique 138	
				Technique 16		Technique 25	Technique 46	Technique 63		Technique 84	Technique 96	Technique 110	Technique 121	Technique 139	
						Technique 26	Technique 47	Technique 64		Technique 85	Technique 97	Technique 111	Technique 122	Technique 140	
						Technique 27	Technique 48	Technique 65		Technique 86	Technique 98	Technique 112	Technique 123	Technique 141	
						Technique 28	Technique 49	Technique 66		Technique 87	Technique 99	Technique 113	Technique 124	Technique 142	
						Technique 29	Technique 50	Technique 67		Technique 88	Technique 100	Technique 114	Technique 125	Technique 143	
						Technique 30	Technique 51	Technique 68		Technique 89	Technique 101	Technique 115	Technique 126	Technique 144	
						Technique 31	Technique 52	Technique 69		Technique 90	Technique 102		Technique 127	Technique 145	
						Technique 32	Technique 53	Technique 70			Technique 103		Technique 128	Technique 146	
						Technique 33	Technique 54	Technique 71			Technique 104		Technique 129	Technique 147	
						Technique 34	Technique 55	Technique 72					Technique 130		
						Technique 35	Technique 56	Technique 73					Technique 131		
						Technique 36	Technique 57	Technique 74					Technique 132		
						Technique 37		Technique 75					Technique 133		
						Technique 38									
						Technique 39									
						Technique 40									

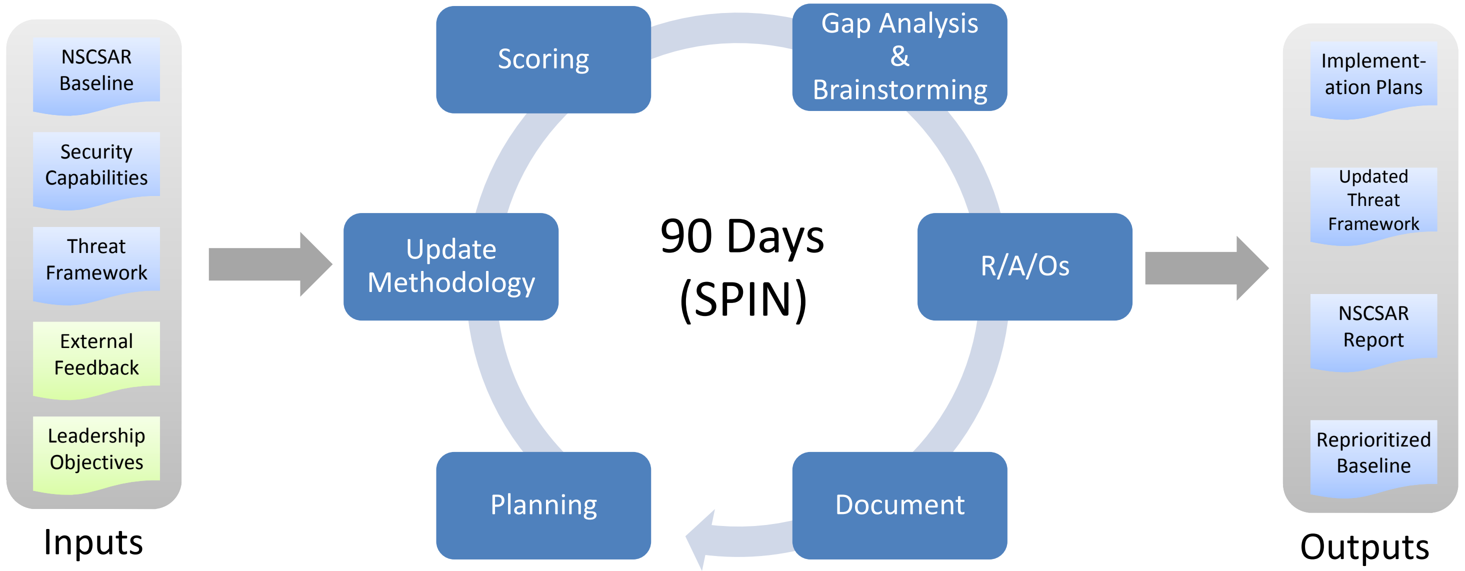
'As-Architected' DoDIN Security Capabilities (Example)



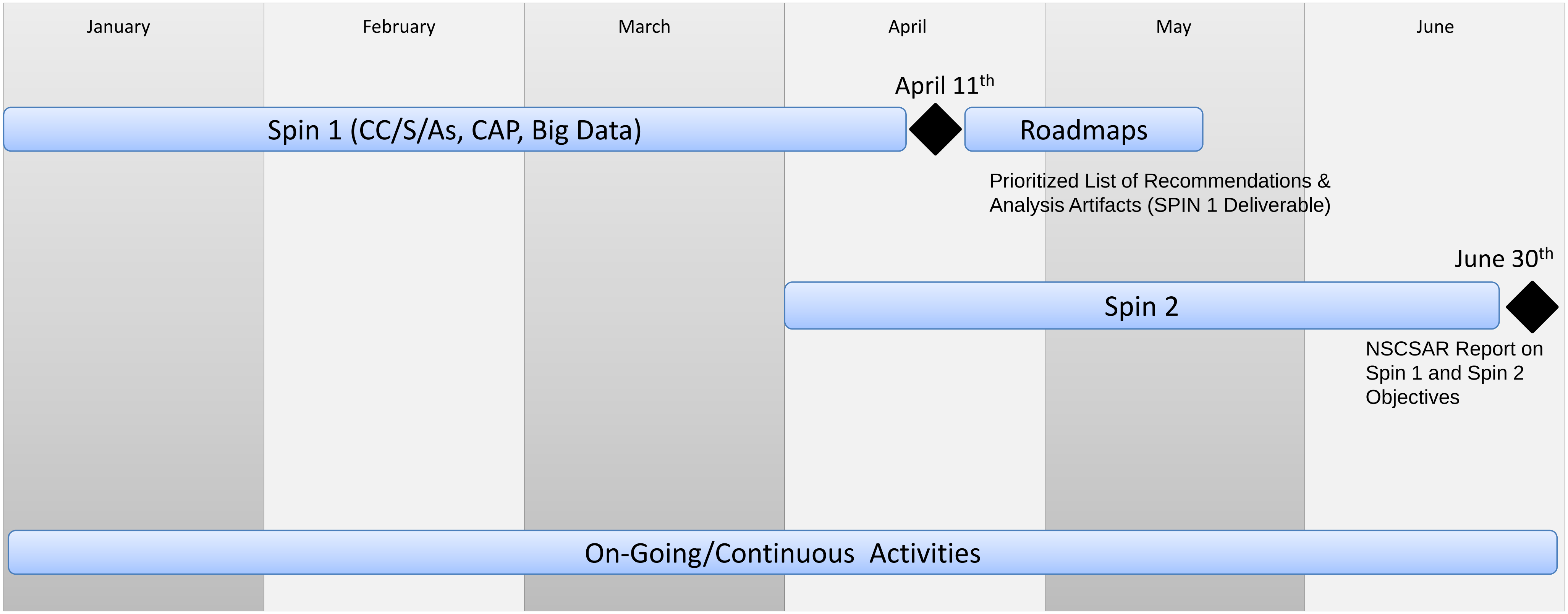
Phase 1			Phase 2			Phase 3								Phase 4	
Tactic 1	Tactic 2	Tactic 3	Tactic 4	Tactic 5	Tactic 6	Tactic 7	Tactic 8	Tactic 9	Tactic 10	Tactic 11	Tactic 12	Tactic 13	Tactic 14	Tactic 15	Tactic 16
Technique 1	Technique 2	Technique 7	Technique 8	Technique 11	Technique 17	Technique 20	Technique 41	Technique 58	Technique 76	Technique 79	Technique 91	Technique 105	Technique 116	Technique 134	Technique 148
	Technique 3		Technique 9	Technique 12	Technique 18	Technique 21	Technique 42	Technique 59	Technique 77	Technique 80	Technique 92	Technique 106	Technique 117	Technique 135	Technique 149
	Technique 4		Technique 10	Technique 13	Technique 19	Technique 22	Technique 43	Technique 60	Technique 78	Technique 81	Technique 93	Technique 107	Technique 118	Technique 136	Technique 150
	Technique 5			Technique 14		Technique 23	Technique 44	Technique 61		Technique 82	Technique 94	Technique 108	Technique 119	Technique 137	
	Technique 6			Technique 15		Technique 24	Technique 45	Technique 62		Technique 83	Technique 95	Technique 109	Technique 120	Technique 138	
				Technique 16		Technique 25	Technique 46	Technique 63		Technique 84	Technique 96	Technique 110	Technique 121	Technique 139	
						Technique 26	Technique 47	Technique 64		Technique 85	Technique 97	Technique 111	Technique 122	Technique 140	
						Technique 27	Technique 48	Technique 65		Technique 86	Technique 98	Technique 112	Technique 123	Technique 141	
						Technique 28	Technique 49	Technique 66		Technique 87	Technique 99	Technique 113	Technique 124	Technique 142	
						Technique 29	Technique 50	Technique 67		Technique 88	Technique 100	Technique 114	Technique 125	Technique 143	
						Technique 30	Technique 51	Technique 68		Technique 89	Technique 101	Technique 115	Technique 126	Technique 144	
						Technique 31	Technique 52	Technique 69		Technique 90	Technique 102		Technique 127	Technique 145	
						Technique 32	Technique 53	Technique 70			Technique 103		Technique 128	Technique 146	
						Technique 33	Technique 54	Technique 71			Technique 104		Technique 129	Technique 147	
						Technique 34	Technique 55	Technique 72					Technique 130		
						Technique 35	Technique 56	Technique 73					Technique 131		
						Technique 36	Technique 57	Technique 74					Technique 132		
						Technique 37		Technique 75					Technique 133		
						Technique 38									
						Technique 39									
						Technique 40									

Built with Dummy Data as Capability/Threat Scoring Aggregation is Classified

General NSCSAR Spin Concept



High Level Spin 1 & 2 Schedule



January

February

March

April

May

June

April 11th

Spin 1 (CC/S/As, CAP, Big Data)

Roadmaps

Prioritized List of Recommendations & Analysis Artifacts (SPIN 1 Deliverable)

June 30th

Spin 2

NSCSAR Report on Spin 1 and Spin 2 Objectives

On-Going/Continuous Activities

Major Spin 1 Objectives

- Expanded Threat Framework ‘Version 1.1’
- Evaluate Additional Security Capabilities
- Score and Analyze all Security Capabilities Against Threat Framework V 1.1
- Updated List of R/A/Os and Analysis Artifacts (no report)

Summary

- NSCSAR Spin 0 Recommendations, Affirmations, and Observations (R/A/O) report available on SIPRNet (classification SECRET)
- Spin 0 R/A/Os driving investment planning for NIPRNet based on DoD's current and future effectiveness at mitigating adversary techniques in the Threat Framework
- Spin 1 underway