NIPRNet/SIPRNet Cyber Security Architecture Review

21 April 2016

NSCSAR

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 United 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

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

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

**Combatant Commanders – Services – Agencies**

- ESSG
- DoD CIO
- CCWG
- JTSO
- JIE EXCOM
- USCC
- JTRB-SA
- IDT
- JIE PCC
- JFHQ DoDIN
- CSLB
- ESDP
- EASB
- EAEP

**UNCLASSIFIED**

- Information Inputs
- Information Inputs and Directly Affects Decision Making
Cyber Security Capabilities

- Perimeter
- Midpoint
- CC/S/As
- Endpoint

Threat Framework

- Pre-Event
- Get In
- Stay In
- Act

Tactics

Heat Maps – Intrusion Sets – Use Cases

Capability Mitigation Scoring

- Pre-Event
- Tactic

Technique

Perimeter
- Protect
- Detect
- Respond

Capabilities

Significant – Moderate – Little

R/A/Os

- Capability Coverage Maps
- Scenarios – Gaps – Redundancies

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

Priority Areas

Paradigm Shifts

Implementation Plans
Threat Framework Example

‘As-Is’ DoDIN Security Capabilities (Example)

‘As-Architected’ DoDIN Security Capabilities (Example)

Built with Dummy Data as Capability/Threat Scoring Aggregation is Classified
# High Level Spin 1 & 2 Schedule

<table>
<thead>
<tr>
<th>January</th>
<th>February</th>
<th>March</th>
<th>April</th>
<th>May</th>
<th>June</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spin 1 (CC/S/As, CAP, Big Data)</td>
<td></td>
<td></td>
<td></td>
<td>Roadmaps</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Prioritized List of Recommendations &amp; Analysis Artifacts (SPIN 1 Deliverable)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>June 30th</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Spin 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NSCSAR Report on Spin 1 and Spin 2 Objectives</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>On-Going/Continuous Activities</td>
<td></td>
</tr>
</tbody>
</table>

- **April 11th**: Roadmaps
- **June 30th**: NSCSAR Report on Spin 1 and Spin 2 Objectives
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