



SPAWAR FLEET READINESS DIRECTORATE (SPAWAR)



Acquisition Research Panel #9: Enabling Cybersecurity

26 APR 2017

Naval Postgraduate School
Acquisition Research Symposium

Rear Admiral John W. Ailes
Deputy Commander
Space and Naval Warfare Systems Command
(SPAWAR)
Fleet Readiness Directorate



Agenda

Topic	Presenter	Time
Introduction of Presenters	RDML Ailes	1530 – 1535
Chair's Opening Remarks	RDML Ailes	1535 – 1545
<i>Cybersecure Modular Open Architecture Software Systems for Stimulating Innovation</i>	Walt Scacchi	1545 – 1600
<i>Security Measurement – Establishing a Confidence that System and Software Security is Sufficient</i>	Carol Woody	1600 – 1615
<i>Decision Support for Cybersecurity Risk Assessment</i>	Hanan Hibshi	1615 – 1630
Q & A		1630 – 1700



Presenters

CHAIR

RDML John W. Ailes, USN
Deputy Commander, Space and Naval Warfare Systems
Command (SPAWAR)
Fleet Readiness Directorate

PRESENTERS

▼ **Dr. Walt Scacchi**

- University of California, Irvine
 - *Cybersecure Modular Open Architecture Software Systems for Stimulating Innovation*

▼ **Dr. Carol Woody**

- Software Engineering Institute
 - *Security Measurement – Establishing a Confidence that System and Software Security is Sufficient*

▼ **Hanan Hibshi (Ph.D. student)**

- Carnegie Mellon University
 - *Decision Support for Cybersecurity Risk Assessment*



Fleet Approach to Cybersecurity

Cyber as a Warfare Mission Area

Leading to Certification

Culture on the waterfront

Cyber Department Heads

Common Reporting Process

Continuous Monitoring

Delivery of fully patched Cyber Baselines

Configuration Managed

Cyber Tool Optimization

Bandwidth,
Patch Distribution,
Network Mapping,
Scan Ranges

Training

Formal Training
Courses PQS to instill
proficiency

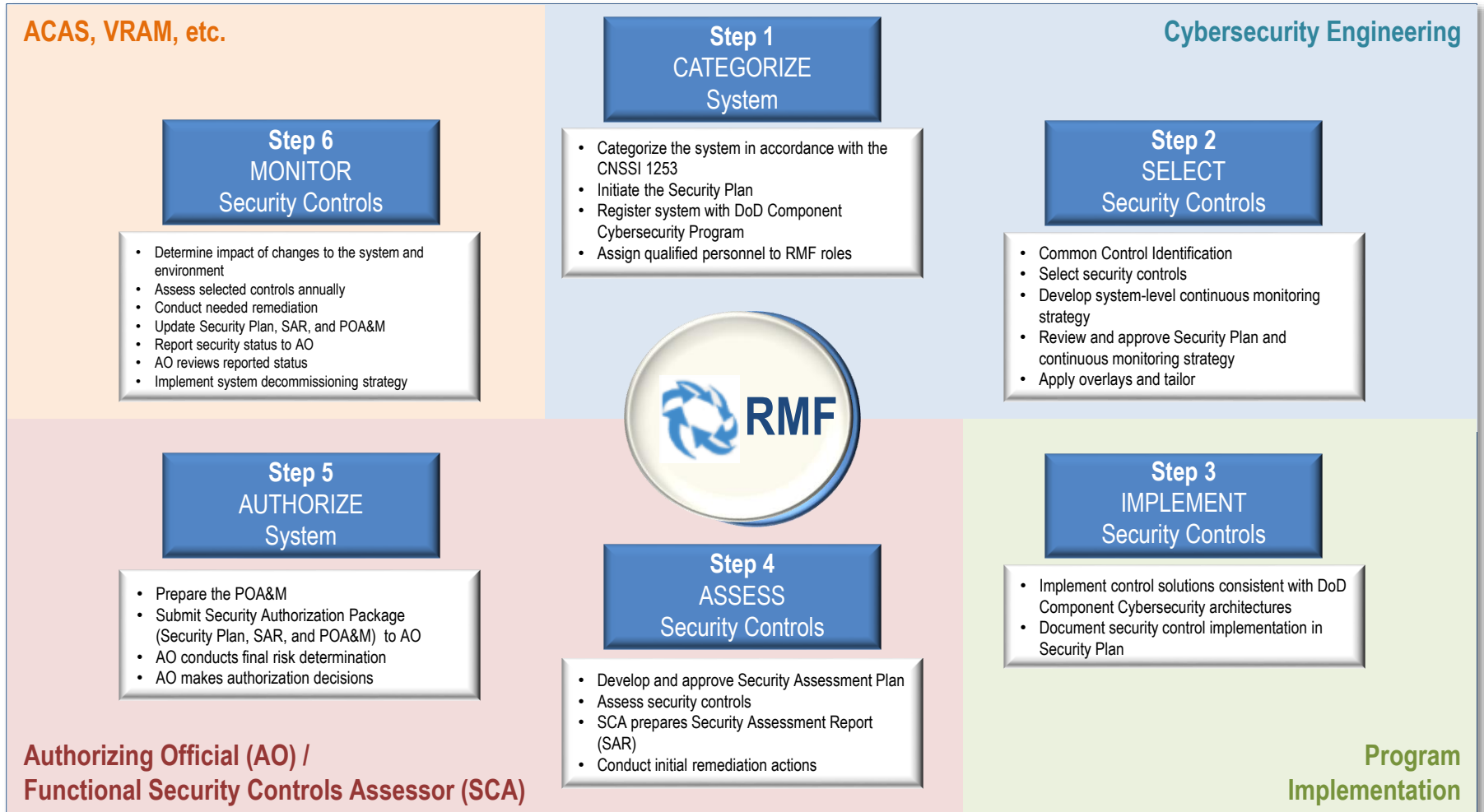
Progress Indicators

- ▼ Scan and patch focus
- ▼ Delivering cyber baselines
- ▼ Created vulnerability dashboard
- ▼ Cyber Warfare established as new mission area in revised Surface Force Readiness Manual
- ▼ Created personal qualifications standards
- ▼ Cyber training courses established
- ▼ Placing engineers onto ships



Risk Management Framework

Process Overview



Risk Management Framework Intended to Provide Greater Insight into Cyber Risk



CYBERSAFE Certification

CS Enclave Design Certification(s)

+

- DFIA compliance
- "Platform" Cyber Test Plan
- "Platform" Boundary Security Policy

=

CS Platform Certification

Integrated into proven platform Certs (NWSCP, Airworthiness) with additional CS assurance

CS System Design Certification(s)

+

- DFIA compliance
- "Enclave" Cyber Test Plan
- "Enclave" Boundary Security Policy

=

CS Enclave Design Certification

In alignment with DFIA and SoS architectural view

CYBERSAFE Risk Assessment with penetration testing

+

RMF

=

CS System Design Certification

RMF with additional CS assurance

Leverage Existing, Proven Processes to the Maximum Extent Possible



IA Standards Designed to Disrupt Cyber Kill Chain

Roadmap to IA TA Standards Development

Most standards enable disruption of multiple steps in the Kill Chain



Standards Completion Status

Current Status

Phase		FY15							FY16							FY17																				
		HLP	Network Firewall	IDPS	ISCM	SIEM	Vulnerability Scan	Boundary Protect	OS	Cyber Risk	TSN	Cyber SA	IT Asset Mgmt	Account Mgmt	Cyber CM	Web Security	Cross Domain Solution	Email Security	Software Assure	RAS	Patch Mgmt	BIOS	IdAM	Event Mgmt	Info Mgmt	PKE	Wireless Comms	WEAC	Data in Transit	Data at Rest	Key Mgmt Exchange	DNS	Virtual Security	Cloud Security	Unified Capability	Support Equipment
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
Discover	Data Gathering / Target Identification																																			
	15/35 Stds			●	●					●	●	●			●	●		●								●		●	●	●		●				●
Probe	Identify Vulnerabilities / Scanning	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	24/35 Stds	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Penetrate	Gain Access / Create Foothold	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	29/35 Stds	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Escalate	Gain Escalated Privileges / Root Access	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	22/35 Stds	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Expand	Multiple Footholds / Paths / Backdoors	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	24/35 Stds	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Persist	Obfuscate Presence	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	16/35 Stds	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Execute	Exploit / Exfiltrate / Attack to Achieve Objective	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	24/35 Stds	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●



Cybersecurity Dashboard

Cybersecurity Readiness Report

PERSPECTIVE: Site Group

SITE GROUP: NAME

VIEW: Summary

Cybersecurity Readiness Report

1 ⓘ

Site	Scan Periodicity ⓘ	Assets Scanned ⓘ	Scan Integrity ⓘ	Unassigned Assets	Current AV Definitions ⓘ	Vulns/Asset (Site Owned) ⓘ	Vulns/Asset (POR Owned) ⓘ	Vulns/Asset (Inv Req'd) ⓘ	Vulns/Asset (All) ⓘ
USS SHIP	10 / 10	123 / 124 (99.2%)	99.2%	0	15 / 116 (12.9%)	4.52	19.93	4.12	28.58
USS SHIP	4 / 12	105 / 106 (99.1%)	97.2%	99	97 / 99 (98%)	1.48	117.93	1.96	121.37
USS SHIP	6 / 10	106 / 198 (53.5%)	50.0%	0	95 / 174 (54.6%)	4.96	18.62	0.99	24.59
USS SHIP	10 / 10	1024 / 1050 (97.5%)	94.7%	31	562 / 624 (90.1%)	2.69	12.59	0.85	16.15
USS SHIP	9 / 10	132 / 133 (99.2%)	96.2%	0	6 / 124 (4.8%)	0.33	11.16	0.65	12.14
USS SHIP	7 / 9	124 / 139 (89.2%)	87.8%	0	93 / 109 (85.3%)	2.21	17.28	0.75	21.26
USS SHIP	7 / 10	89 / 98 (90.8%)	88.8%	0	76 / 83 (91.6%)	9.93	22.42	7.19	39.54
USS SHIP	10 / 12	140 / 140 (100%)	95.0%	6	113 / 118 (95.8%)	6.07	23.39	2.05	31.51
USS SHIP	9 / 9	134 / 134 (100%)	99.3%	0	113 / 113 (100%)	1.76	11.75	0.57	14.11

Vulnerability per Asset:

Green: Less than 2.5

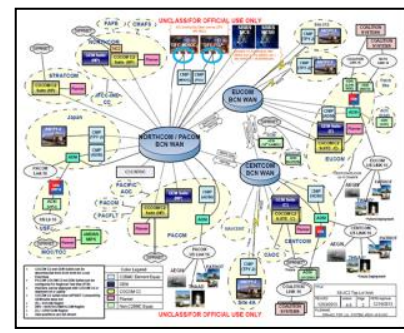
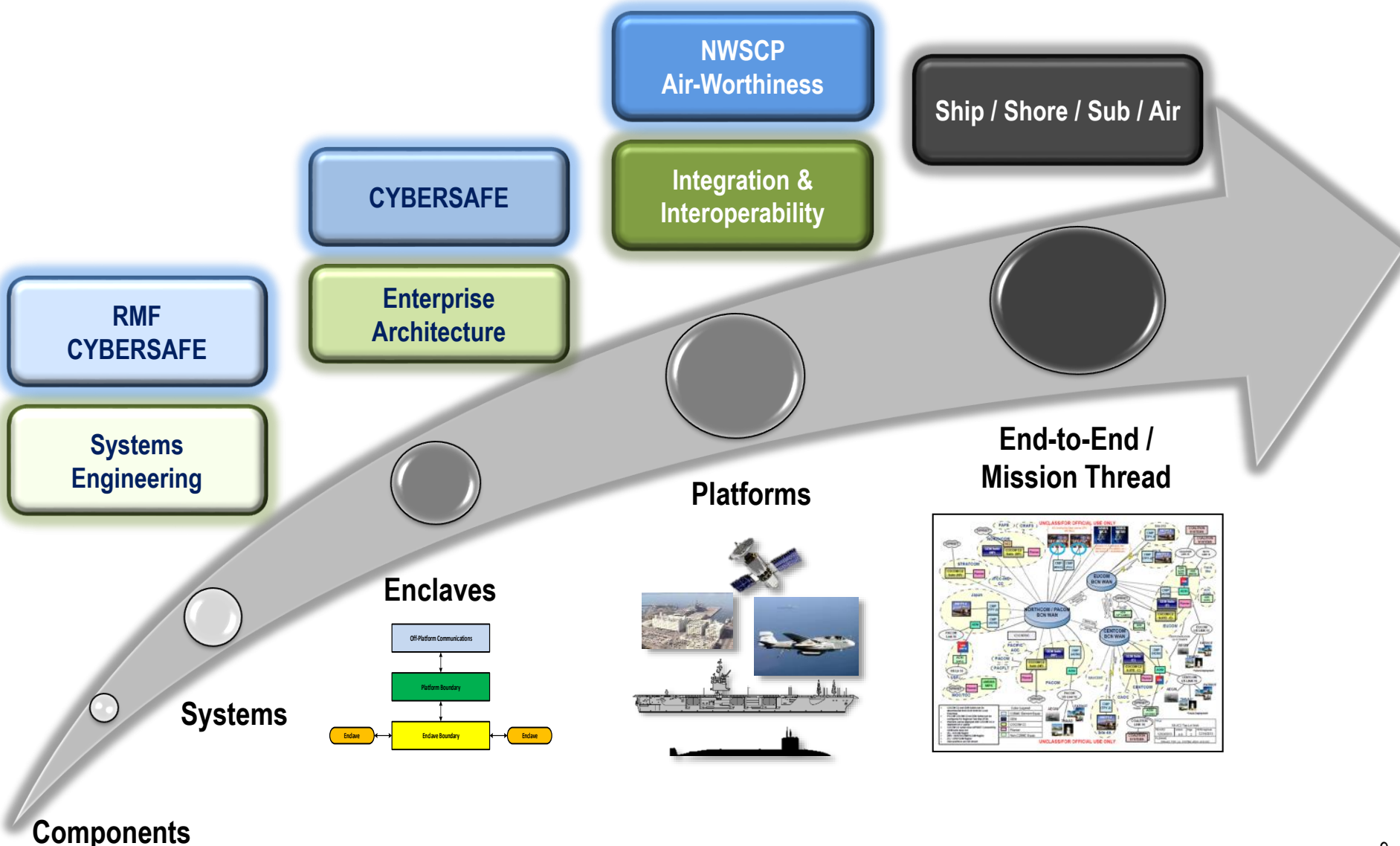
Yellow: Greater than or equal to 2.5, but less than 3.5

Red: Greater than 3.5

Ship's Force Responsibility

Program of Record Responsibility

Holistic Approach to Cyber Security





Presenters

CHAIR

RDML John W. Ailes, USN
Deputy Commander, Space and Naval Warfare Systems
Command (SPAWAR)
Fleet Readiness Directorate

PRESENTERS

▼ **Dr. Walt Scacchi**

- University of California, Irvine
 - *Cybersecure Modular Open Architecture Software Systems for Stimulating Innovation*

▼ **Dr. Carol Woody**

- Software Engineering Institute
 - *Security Measurement – Establishing a Confidence that System and Software Security is Sufficient*

▼ **Hanan Hibshi (Ph.D. student)**

- Carnegie Mellon University
 - *Decision Support for Cybersecurity Risk Assessment*