

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

**AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA**

Driving Ongoing Authorization (OA) with Good Cyber Practices

How to Be Cyber Ready Beyond Your Inspection

LCDR K Neill Miller, Mr. Robert Beady, and Mr. Robert Talbot



Speaker Introduction

LCDR K. Neill Miller

US Navy: *RME Cybersecurity Lead, CHRIP Section Chief, CROSS Section Chief*

Mr. Robert Beady

DHA: SCA

Mr. Robert Talbot

NIWC: *CHRIP Execution Lead, OA Execution Lead*

Agenda

- 1** Cyber Health and Readiness Inspection Program (CHRIP) compared to Ongoing Authorization (OA)
- 2** The Measures of Performance (MOPs)
- 3** The OA Scoring System
- 4** OA Planning and Sustainment
- 5** Enhanced Continuous Monitoring (eCM)

Learning Objectives

1. Discuss How CHRIP Informs and Prepares for OA
2. Identify the Most Challenging MOPs
3. Illustrate How to Plan for MOP Execution and Paths to Success
4. Define the MOPs Most Critical to the Maintenance of OA Scores
5. Highlight Strategies in Maintaining Compliance
6. Explain How eCM Differs from Previous Methods
7. Discuss How eCM practices will assist with OA Entry

Overview

- The Continuous Monitoring (CM) process and its tools have matured to a point where they can be used to measure compliance scoring in a more robust and timely fashion
- Source data from enterprise tools is available in Splunk to allow for Measure of Performance (MOP) automation
- All Military Treatment Facilities (MTFs) will transition to an Enhanced Continuous Monitoring (eCM) methodology and harness the increased capabilities in the near future
- eCM's baseline data set and scoring model enables the implementation of Ongoing Authorization
 - Data on the eCM dashboard is updated daily and looks back over the last 7-days

Cyber Health and Readiness Inspection Program (CHRIP)

- CHRIP – an Inspection and Assessment Program
 - Occurs once every 3 years
 - Lasts for 5 Weeks + 90 Days
 - +1700 MOPs covered during assessment
 - Prepares for OA and Verifies OA Status as Independent Verification & Validation (IV&V)
 - Supports preparation for Enhanced Continuous Monitoring (eCM)
 - Views requirements as holistic patterns

Ongoing Authorization (OA)

- OA – an Extension to your Authorization
 - Focus remains on Sustainment
 - 33 MOPs
 - 20 MOPs are used for scoring
 - 16 are scored weekly; and 4 quarterly
 - 15 are automated; 5 are manual
 - 13 other MOPs are provided for Informational/Diagnostic purposes
 - Repeated patterns of action are key

Enhanced Continuous Monitoring (eCM)

- eCM – a form of constant Risk Posture Assessment
 - Enables OA by providing timely compliance data
 - Sustainment remains the focus
 - Requirement timeframes are near/short term
 - 15 MOPs Total
 - All 15 MOPs are used for Scoring
 - All 15 are automated
- The 5 Manual MOPs used in OA are NOT in eCM
- Repeated patterns of action remain the key

eCM – Maturing Continuous Monitoring

- eCM provides greater granularity and visibility to identify the individual components of your score
- Leverages a wider range of sources
 - Direct transition from CM to eCM
 - Overall Vulnerability Scan Score
 - Credentialed Scan coverage
 - CSSP Tools Compliance
 - Assessment Procedures
 - MECM
 - ESS
 - Additional data for eCM
 - BitLocker Status
 - End of Life Operating System and Applications
 - Critical and High Vulnerabilities over 21 days old
 - POA&M Status and Monitoring
 - Account Least Privileged
 - ACAS Configuration and Scan Upload to eMASS
- Automated MOP Values are Updated Daily
 - Evaluation Range is Previous 7 Days

eCM is Built to Mature

- Enterprise tools update and change over time
 - Dashboard/Scoring is flexible
 - Adapted for transition from Trellix to Microsoft Defender
 - Future planning - CrowdStrike

Additional Robust Features

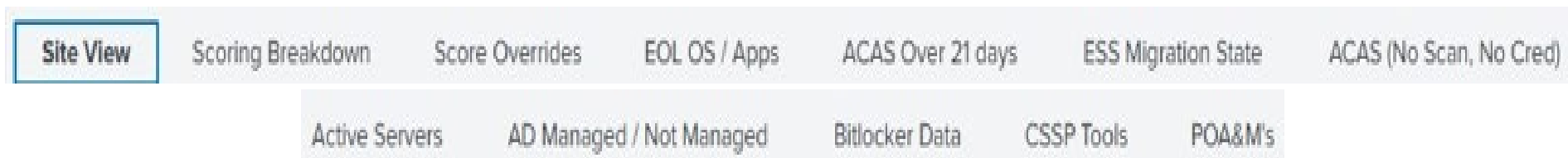
- POA&M data is pulled from eMASS and mapped to Vulnerabilities
 - A POA&M must be an Approved or Risk Accepted
 - Findings with POA&Ms are not counted against the site

Criticals Over 21 Days ACAS-13	Highs Over 21 Days ACAS-14	Criticals	Highs	Mediums	Lows
42	83	85	252	2,992	20
Criticals, Highs Over 21 days Mitigated with POAM or RA		Criticals, Highs, Mediums, Lows Mitigated with POAM or RA			
0	191	7	330	598	1

Do not POA&M for a vulnerability if the mitigation/remediation does not degrade or inhibit system functions

eCM is Also More Transparent

- Data on the dashboard provides actionable details
 - Hosts with Vulnerabilities (ACAS Over 21 days)
 - Software EOL and missing components (EOL OS/Apps)
 - ACAS Details (ACAS (No Scan, No Cred)
 - Active Directory (Active Servers, AD Managed/Not Managed)
 - Tools Data (ESS Migration State, BitLocker Data, CSSP Tools)
 - POA&M Details (POA&Ms)
 - Scoring Details (Scoring Breakdown and Score Overrides)



Robustness and Transparency for ACAS 13/14

- ACAS Over 21 Days tab on dashboard
 - Displays Plugin Name and Hosts Affected
 - Critical/High Vulnerabilities over 21 Days old without a POA&M
- Assists in identifying upcoming issues
 - Plugins and Host getting close to the 21-day threshold

EOL OS / Apps **ACAS Over 21 days** ESS Migration State

Criticals Currently >21 Days that do not have POAM or RA			Upcoming Vulnerabilities				
Plugin Name	Number Affected	Host(s) Affected	Host	Plugin Name	Vuln Age	First Seen (Days)	Days Till Accountable
Google Chrome < 148.0.7778.167 Multiple Vulnerabilities	13	BAEYWK2036SFB	BAEYWK4MLPGT3	Google Chrome < 148.0.7778.216 Multiple Vulnerabilities	43	16	5
		BAEYWK2036SFR					
		BAEYWK4LLPGT3					
		BAEYWK5FQ10M2					
		BAEYWK82VBLR2					
		BAEYWK82VDLR2					
		BAEYWK82XFLR2					
		BAFYWK827RI R2					
			BAEYWK4MLPGT3	Google Chrome < 149.0.7827.53 Multiple Vulnerabilities	37	16	5

Knowledge Check 1

True or False:

- Requirements are adhered to only for the assessment period to meet catch-up goals.

Knowledge Check 1 - Answer

True or False:

- Requirements are adhered to only for the assessment period to meet catch-up goals.

FALSE

OA vs eCM MOP Applicability and Threshold

- Authorization Status determines the Set scorable MOPs
 - MTFs in OA will be scored based on all 20 MOPs
 - MTFs not in OA will be scored based on 15 of the 20 MOPs (5 manual MOPs are marked N/A)
- All MTFs, regardless of Authorization status, are scored the same way
- The Cumulative Score <70 is Considered Critical

Cumulative Score Ranges ↕	Risk ↕
< 70	Critical
70 - 79.99	Significant
80 - 88.99	Escalated
89 - 91.99	Moderate
92 - 94.99	Minimal
95 - 100	No Concern

Why Does OA and eCM Use Raw and Scale Points?

- Flexibility when tools or requirements change
 - Change Raw Point assignments without having to overhaul the entire scoring system
 - Adjust focus to different requirements
 - Transition to new tools more easily
- Scale Points give us a clear overall scoring range
 - There are always 100 Scale points
- Raw Points allow us to shift weight between MOPs
 - Raw Point to Scale Point Ratio is 3.2 to 1
 - Currently there are 252 Raw Points
 - MOPs are assigned Raw Points, not Scale Points

Thresholds Scoring

- Most of the Scorable MOPs have two score thresholds
 - Full Points Threshold = All Raw Points are earned at or above that value
 - Zero Points Threshold = no Raw Points are earned at or below that value

ACAS				
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points
ACAS Vuln Score (ACAS-12)	40	0.5	2.5	0.20
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points
Cred Scan % (ACAS-08)	20	95%	85%	2.00

- You earn (or retain) an incremental number of Raw Points between those two thresholds
 - You start losing Raw Points when you go below the Full Points Thresholds
 - For Example: if ENS Platform had a recorded score of 94%, then 2 Raw Points would be lost
 - 0.625 Cumulative Score Points are lost (2/3.2)
 - Allows for fine control over impact from recorded value changes

Binary Scoring

- 10 MOPs have directly allocated Raw Points
- All 10 contribute to the Overall Score in OA
- 5 contribute to the Overall Score in eCM
- The requirements do not allow for thresholds

ACAS	
Crits +21 Days (ACAS-13)	-10
Highs +21 Days (ACAS14)	-10
No False Positive Reporting (CS04)	-4
eMASS and System State	
ACAS Scans Not Imported (VMP10)	-6
AD Accounts Violate Least Privilege (UAC13)	-10
POA&Ms +90 Days Overdue (VMP02)	-6
Open ACAS Vulnerabilities (no POA&M) (VMP11)	-6
POA&Ms Not Updated in 90 Days (VMP03)	-6
End of Life/End of Support Issues	
EoL/EoS OSs (EOL03)	-6
EoL/EoS Applications (EOL04)	-6

Points to Consider

- Not every CHRIP MOP is in the OA/eCM dashboard
 - Only the most impactful ones are included
- Every CHRIP MOP is assessed during a CHRIP assessment
 - CHRIP is IV&V for OA
 - OA/eCM MOPs are based on CHRIP MOPs
- Even if/when tools change, the foundational requirements seldom change

The 6 Most Challenging OA/eCM MOPs

- Most common findings:
 - 1) ACAS-12: Vulnerability score too high
 - 2) ACAS-13: Critical Vulnerabilities still present 21 days past discovery
 - 3) ACAS-14: High Vulnerabilities still present 21 days past discovery
 - 4) CND-08: BitLocker not active and fully encrypting
 - 5) DHA-EOL03: Assets with End-of-Life/End-of-Support Applications
 - 6) DHA-EOL04: Assets with End-of-Life/End-of-Support Operating Systems
- Initial findings in nearly all CHRIP Assessments

How Do These 6 MOPs Affect OA, eCM, or CHRIP?

- Significant impact when combined
 - 92 out of 252 raw points lost just from 6* MOPs
 - ACAS-12 = 40
 - CND08 = 20
 - ACAS-13 and ACAS-14 = 20 combined
 - DHA-EOL03 and DHA-EOL04 = 12 combined
 - 28.75 out of 100 scale points
 - $92/3.2 = 28.75$

Knowledge Check 2

- What Are The 2 Measures of Performance (MOPs) Often Seen As the Most Difficult?
 - a. The 50 and 100 MOP Dashes in the Pre-Assessment
 - b. SAAR90 and Cyber Awareness-001
 - c. ACAS-13 and ACAS-14
 - d. CAC Sweeps and OPSEC Self Assessments

Knowledge Check 2 - Answer

- What Are The 2 Measures of Performance (MOPs) Often Seen As the Most Difficult?
 - a. The 50 and 100 MOP Dashes in the Pre-Assessment
 - b. SAAR90 and Cyber Awareness-001
 - c. ACAS-13 and ACAS-14
 - d. CAC Sweeps and OPSEC Self Assessments

The Nature of The 6 MOPs

- Root Causes of Challenges:
 - ACAS-12, 13 and 14
 - Scan results not proactively monitored week-over-week to address vulnerabilities
 - CND-08:
 - Weekly BitLocker check not scheduled
 - DHA-EOL03 and 04
 - Enclave content not reviewed against MedCOI architecture or HW/SW list/baseline (similar to ACAS-10)
 - Often paired with PORs improperly placed in enclave and lack of communication with PMOs
 - CM-08 control is changing to require inventory content to be updated whenever there is a change

Strategies for Success (LAMP)

- While there are numerous short-term fixes, CHRIP has found the following to be the most effective strategy for the long-term for OA and eCM:
 - List: itemize each action by timeframe organize accordingly
 - Assign: delegate actions for better communication, workload balance, and action speed
 - Monitor: track the timelines, interactions, changes, and execution of each action
 - Pursue: close the action when complete and follow-up with enforcement as needed
- These steps work concurrently with each other
 - Multiple actions will run at the same time
 - It also works at every scale of operation (from entire year to single requirement)
 - **LAMP** establishes sustainable patterns

Example of Using LAMP

- CND-08 (BitLocker not active and fully encrypted)
 - List:
 - Applicable systems require BitLocker enabled and encrypted drives
 - Assign:
 - Determine who is taking action (who is monitoring BitLocker status?)
 - Is there any special action or messaging that needs to take place for remote machines?
 - Monitor:
 - Is a daily/weekly check of BitLocker status scheduled?
 - Post-update re-enabling and re-encrypting tends to cause shortfalls
 - Pursue:
 - Close actions when complete and follow-up with enforcement as needed
 - POA&M Status and Monitoring
 - Account Least Privileged
 - ACAS Configuration and Scan Upload to eMASS

Knowledge Check 3

- What Intervals Should You Follow For All MOPs and why?
 - a. Weekly and Monthly Because They Are The Shortest Periods
 - b. Weekly and Quarterly Because They Influence Each Other
 - c. Twice a Week To Remain Prepared
 - d. Only at the Interval Stated for Each MOP

Knowledge Check 3 - Answer

- What Intervals Should You Follow For All MOPs and why?
 - a. Weekly and Monthly Because They Are The Shortest Periods
 - b. Weekly and Quarterly Because They Influence Each Other
 - c. Twice a Week To Remain Prepared
 - d. Only at the Interval Stated for Each MOP

Tips to Remember

- Spread out where you can
 - Use long timeframes to your advantage
 - RMF P&P/Control Review can be spread out over a year
- Delegate where you can
 - Don't stovepipe where you don't have to – you will waste resources and fall behind
- Remember some requirements have more than one timeframe
 - Some have rolling timeframes (week-over-week)

Questions



Contacts

LCDR K Neill Miller

RME Cybersecurity Lead
CHRIP Section Chief
CROSS Section Chief



kerry.n.miller2.mil@health.mil

Mr. Robert Beady

SCA



robert.c.beady.civ@health.mil

Mr. Robert Talbot

NIWC: CHRIP Execution Lead
OA Execution Lead



robert.j.talbot.civ@health.mil

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA

Thank You!



UNCLASSIFIED

Backup

Common CHRIP Associations

- All 6 Challenging MOPs often occur with the following during a CHRIP Assessment:
 - ACAS-10: Scanning asset lists incomplete or incorrect
 - DHA-CM09: architecture diagram not up-to-date
 - DHA-CM11: HW/SW baseline not complete/inaccurate
 - DHA-MDE04: site not listed in MDE deployed locations list
 - DHA-CM17: no lifecycle management plan
 - This is the only one that is not a Critical Override

OA/eCM Scoring Breakdown

Score Scale Points	Scale to Raw Point Ratio								
100	3.2								
ACAS									
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points	Recorded Value	Override	Sub- Raw Points Lost	Raw Points Lost	Scale Points Lost
ACAS Vuln Score (ACAS-12)	40	0.5	2.5	0.20	0.00	No	0.00	0.00	0.00
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points	Recorded Value	Override			
Cred Scan % (ACAS-08)	20	95%	85%	2.00	100.00%	No	0.00		
Crits +21 Days (ACAS-13)	10				None Found (Pass)	No	0.00		
Highs +21 Days (ACAS-14)	10				None Found (Pass)	No	0.00		
False Positive Reporting (CS04)	4				Valid False Positives Reported (Pass)	No	0.00		
ESS	ESS Solution(s):	Defender+Trellix							
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points	Recorded Value	Override	Sub- Raw Points Lost	Raw Points Lost	Scale Points Lost
ESS (CND25)	30	95%	85%	3.00	100.00%	No	0.00	0.00	0.00
Bitlocker									
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points	Recorded Value	Override	Sub- Raw Points Lost	Raw Points Lost	Scale Points Lost
Bitlocker (CND08)	20	95%	85%	2.00	100.00%	No	0.00	0.00	0.00
CSSP Tools									
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points	Recorded Value	Override	Sub- Raw Points Lost	Raw Points Lost	Scale Points Lost
Encase (CND01)	10	90%	80%	1.00	100.00%	No	0.00	0.00	0.00
Splunk (CND03)	20	90%	80%	2.00	100.00%	No	0.00		
Sysmon (CND05)	10	90%	80%	1.00	100.00%	No	0.00		
WinEvent Codes (CND07)	10	90%	80%	1.00	100.00%	No	0.00		
MECM									
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points	Recorded Value	Override	Sub- Raw Points Lost	Raw Points Lost	Scale Points Lost
MECM Agent (MECM01)	10	95%	85%	1.00	100.00%	Yes	0.00	0.00	0.00
eMASS and System State									
Component	Raw Points	Full Points Threshold	Zero Points Threshold	Incremental Points	Recorded Value	Override	Sub- Raw Points Lost	Raw Points Lost	Scale Points Lost
Assessment Procedures	10	95%	85%	1.00	100.00%	No	0.00	0.00	0.00
ACAS Scans Imported (VMP10)	6				ACAS Scans Imported (Pass)	No	0.00		
AD Accounts Violate Least Privilege (UAC13)	10				Accounts Do Not Violate Least Privilege (Pass)	No	0.00		
POA&Ms >90 Days Overdue (VMP02)	6				POA&Ms > 90 Days Overdue Are Not Present (Pass)	No	0.00		
Open ACAS Vulnerabilities (w/o POA&M) (VMP11)	6				No Open ACAS Vulnerabilites Present w/o POA&Ms (Pass)	Yes	0.00		
POA&Ms Updated in 90 Days (VMP03)	6				All POA&Ms Have Been Updated In 90 Days (Pass)	No	0.00		
End of Life/End of Support Issues									
Component	Raw Points				Recorded Value	Override	Sub- Raw Points Lost	Raw Points Lost	Scale Points Lost
EoL/EoS Applications (EOL03)	6				No EoL/EoS Applications Found (Pass)	No	0.00	0.00	0.00
EoL/EoS OSs (EOL04)	6				No EoL/EoS OSs Found (Pass)	No	0.00		

A Complex Example of Using LAMP

- ACAS-13 and 14 (Critical and High Vulns 21 Days Past Discovery)
 - List:
 - Vuln Scans are every 7 days and Crits/Highs must be addressed within 21 days
 - There's 2 timeframes and 2 actions (scanning and patching)
 - Assign:
 - Determine who is taking action (who does scans every 7 days, who addresses the vulns within 21 days)
 - Are there so many findings that you need to focus more SAs?
 - Monitor:
 - As you scan every 7 days, remember that new vulns appear that also have 21-day timers.
 - What you closed before comes off your list; new ones rotate onto the list
 - Pursue:
 - Close actions when complete and follow-up with enforcement as needed (reimage or remove asset from network)
- The ultimate result is a Patch Plan (it would cover ACAS-12 also)

A LAMP Example with Varying Timeframes

- DHA-EOL03 and 04 (End-of-Life/End-of-Support Applications and Operating Systems)
 - List:
 - Use your tools to build and verify your HW/SW lists and identify systems with known EOL/EOS
 - *Several tools point out EOL/EOS items, but you need to be proactive*
 - Do you know when they reach EOL/EOS?
 - Are they PORs and has contact been made with the PMOs to establish replacements?
 - Capture the eMASS IDs and ATDs of those PORs
 - Assign:
 - Determine who has cognizance of applications/systems in question
 - *They can help populate the List information and keep it updated*
 - Monitor:
 - Are these applications/systems still present week over week? Do additional EOL/EOS appear?
 - Has action been taken to remove/replace/upgrade them?
 - Pursue:
 - Has the removal/replacement/upgrade action been followed-up and completed?
 - *Sites have a responsibility to see this through (even with PORs)*
- The ultimate result is a basic Lifecycle Management Plan
 - This could be used to address DHA-CM09, CM11, CM17, and MDE04

A Key Aspect of LAMP

- It's a cycle, the four parts always inform and build each other
- For example:
 - Your List should tell you:
 - Who has the assignment
 - What they are doing to monitor
 - What are the actions in pursuit
 - When the requirements must be satisfied
 - When they were actually resolved

