

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

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

Risk Management Executive (RME) Leadership Panel

Mr. Marc Shelton, Maria Cante, LCDR Kerry Miller, David Lima

Moderator: Mr. Richard Gasperoni



Agenda

- 1** RME Leadership Panel – Speaker Introductions
- 2** Learning Objectives
- 3** Live Q&A from the audience

Speaker Introductions



Mr. Marc Shelton

Risk Management Executive,
Division Chief
Defense Health Agency



Ms. Maria Cante

Risk Management Executive
ERM Branch Chief
Defense Health Agency



LCDR Kerry Miller USN

Risk Management
Executive, Cyber Health and
Readiness Inspection Program
(CHRIP) Section Chief, Cyber Security
RMF Operations Support Services
(CROSS) Section Chief
Defense Health Agency



Mr. David Lima

Risk Management Executive,
Cyber Operations Center
(CyOC) Branch Chief
Defense Health Agency



Mr. Richard Gasperoni

Risk Management Executive,
Chief Operations Officer
Defense Health Agency

Learning Objectives

- 1** RME Leadership's vision, direction, and support of the DHA mission in the construct of Combat Support
- 2** Update Cybersecurity Practitioners on the upcoming CrowdStrike tool
- 3** Cybersecurity Maturity Model Certification (CMMC) Efforts
- 4** Discuss efficiencies being found to speed the delivery of cybersecurity approvals.

RME Leadership's Vision, Direction, and Support of the DHA Mission in the Construct of Combat Support

- **Vision:** To be a cornerstone of warfighter readiness by delivering pioneering and resilient cybersecurity and risk management, ensuring the Military Health System's digital infrastructure is a decisive advantage in all operational environments.
- **Mission:** To defend the military health enterprise by proactively identifying and neutralizing cyber threats, streamlining secure technology adoption, and embedding risk management into all operations, thereby directly enabling the lethality, survivability, and readiness of the Joint Force.

New and Improved RME SharePoint Site



[DHA](#) [AD-HC&O](#) [Support, Personnel & Financial Ops](#) [AD-RD&A/CAE](#) [Defense Health Networks](#) [Programs](#) [Site Map](#) [SPO Resources](#)



[Risk Management Executive](#) [Cyber Operations Center](#) [Cyber Policy, Process & Training](#) [Cyber Health Assurance & Support](#) ...



Risk Management Executive

DHA Internal and External Public

☆ [Add to favorites](#)

[Home](#)

[Branches](#) ▾

[Resources & Tools](#) ▾

[RME Town Hall](#)

[Training & Knowledge Services](#) ▾



"Agentic AI is a major evolution in artificial intelligence, moving beyond simple input-output models to systems that can interpret instructions and execute tasks autonomously."



2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM

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

CrowdStrike Tool



RMED Problem Statement

DHA's current security architecture is overly complex, fragmented, and reliant on legacy detection methods, leaving critical healthcare delivery systems and military readiness data vulnerable to sophisticated, identity-based, and cloud-focused adversary attacks.

Area	Core Issue	Impact
High-Value Target	Sophisticated adversaries target DHA's unique mix of military readiness data, sensitive medical info, and operational technology.	Threatens patient care, family welfare, and global military readiness.
Fragmented Defenses	Patchwork of legacy point solutions (HBSS, Microsoft Defender) with poor server coverage, high costs, and disjointed management.	Limits enterprise-wide visibility and hampers coordinated incident response.
Outpaced Detection	Legacy signature-based tools fail against modern "living-off-the-land" tactics and fileless malware.	Sophisticated actors can maintain undetected persistence for months.
Cloud & Identity Risks	Rapid hybrid cloud adoption and complex Active Directory structures create blind spots and credential-based vulnerabilities.	Strict security controls are difficult to enforce without disrupting 24/7 patient care.

How the CrowdStrike Platform Helps

Unified Architecture

- Cloud-native platform delivering comprehensive threat prevention, detection, and response.

Advanced Protection

- Integrates endpoint security, cloud analytics, and autonomous local processing.

DHA Mission Alignment

- Meets Defense Health Agency requirements for continuous security operations.

Operational Resilience

- Ensures consistent protection across connected, disconnected, and air-gapped environments.

Autonomous Design

- Leverages cached intelligence and local processing to prevent degradation during network interruptions.

How the CrowdStrike Platform Helps

The CrowdStrike platform will provide you with a powerful, consolidated toolkit to help align Risk Management activities and enhance security management. Enabling prioritized action directly within your area of responsibility.

Command Your
Security Posture

- Gain a single, real-time dashboard showing the health of all your endpoints.
- Move from reactive to proactive risk management
- Enabling the prioritization of your most critical exposures.

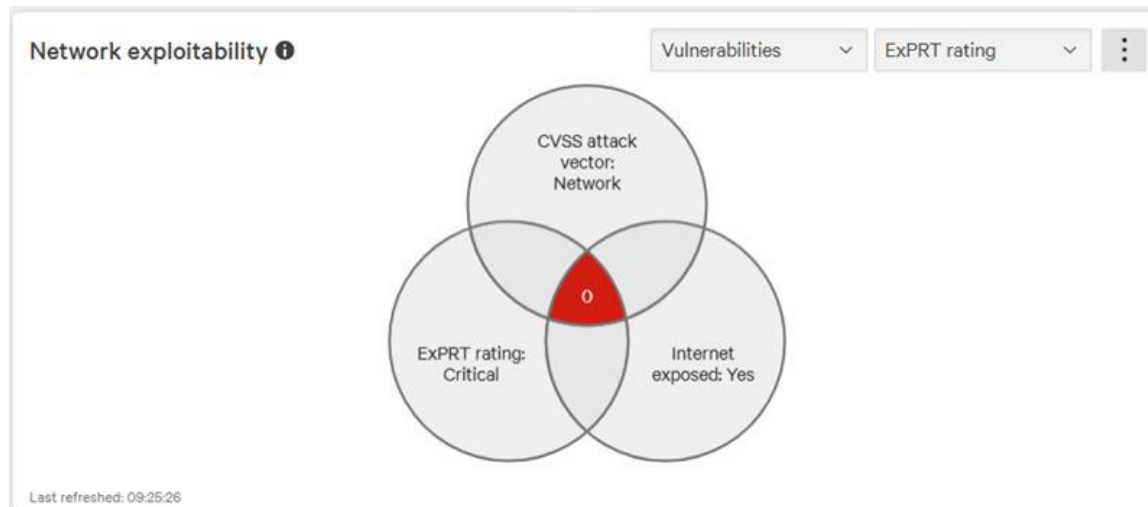
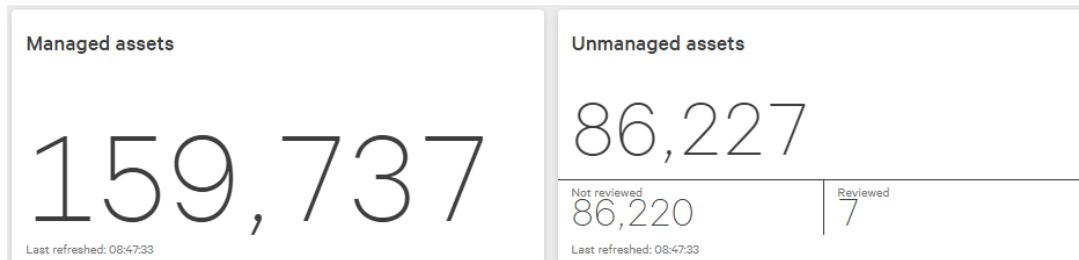
Streamline Audits
and Compliance

- Drastically reduce audit preparation time. The platform provides on-demand access to compliance status and the granular data needed to satisfy audit requirements, turning a stressful event into a routine report.

Master Your Assets
and Identities

- Visibility of assets and identities on your network.
- Ability to hunt for identity-based threats and enforce IT hygiene
- Identify unmanaged devices or unauthorized applications that exist in your environment.

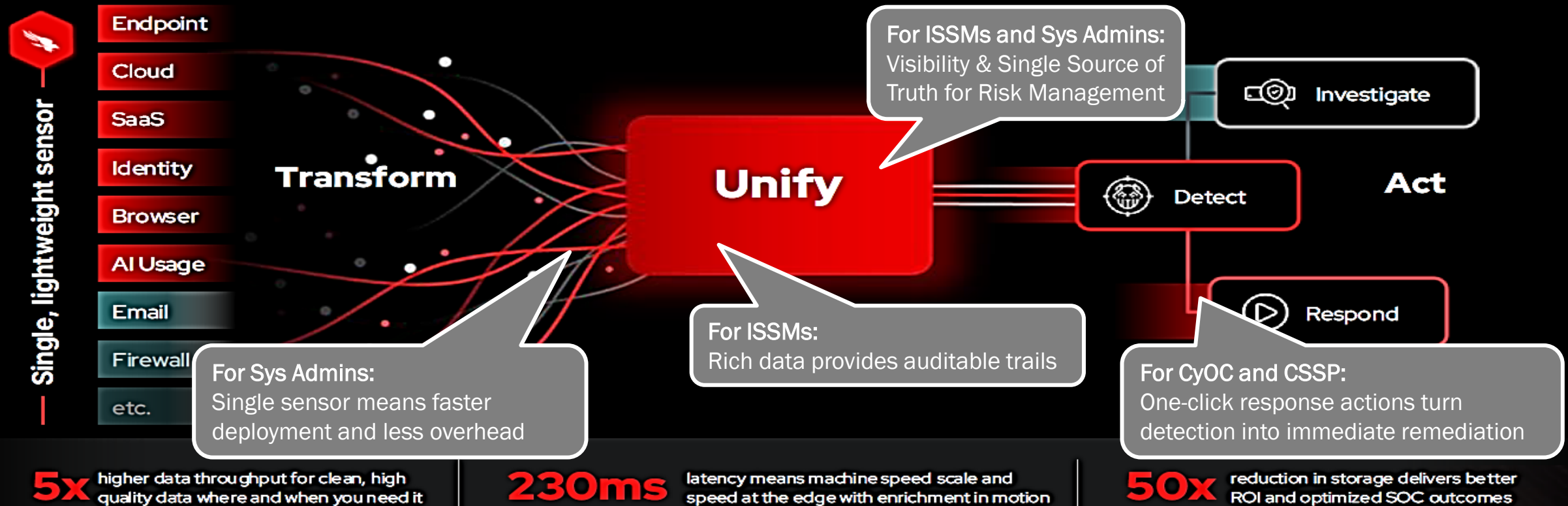
Where We are Today



Unified Control: One Sensor, Complete Team Integration

Your Unified Defense System

One sensor. One console. One platform.



Where We are Going

Unifying DHA Enterprise visibility and Risk Management through the consolidation and simplification of Endpoint Security Solution (ESS), Endpoint Detection and Response (EDR), Vulnerability Identification and Management, Assess and Authorization.

Unified Security Operations

- Ensure alignment between CyOC, CROSS, ERM, and Operational Field through single source of truth for endpoint security posture

Enhanced Visibility

- Aligns asset compliance views to help identify previously unmanaged assets or risks
- Real-time visibility into insider and adversarial activity

Simplified Management

- Single Agent Deployment
- Single interface for policy, exclusions, and suppressions
- Streamlines system access and training

Improved System Performance

- The lightweight agent minimizes CPU/memory impacts
- Scalable SaaS offering

2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM

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

Cybersecurity Maturity Model Certification (CMMC)



Cybersecurity Maturity Model Certification (CMMC)

- The fundamental purpose of the Cybersecurity Maturity Model Certification (CMMC) relative to Department of War (DoW) IT is to secure the enterprise's extended attack surface: the Defense Industrial Base (DIB).
- While DoW IT systems are governed by frameworks like NIST SP 800-53 and FedRAMP, CMMC ensures that when Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) leave DoW networks and enter contractor systems, that data is protected to a verifiable standard. It translates existing cybersecurity requirements—specifically NIST SP 800-171—into a standardized assessment model that contractors must meet to do business with the Department.

CMMC – Bottom Line

- Phased Enforcement is Active - With final rules enacted in late 2025, CMMC is no longer theoretical. Independent third-party certification is actively scaling as a strict, non-negotiable condition for contract awards across the Defense Industrial Base. **PAUSED**
- From Trust to Verification - The era of self-attestation is effectively over. Mandatory C3PAO assessments and senior executive affirmations in SPRS now carry severe, boardroom-level legal liabilities under the False Claims Act. **PAUSED**
- Strict 180-Day Remediation - Open-ended vulnerabilities are eliminated.
- Any non-critical deficiencies permitted on a Plan of Action and Milestones (POA&M) face a rigid 180-day deadline before certification—and associated contracts—are revoked.

CMMC - Basics

What is CMMC?

Unified DoW framework to ensure contractors (and DHA programs) implement adequate cybersecurity controls for FCI and CUI — in practice, not just on paper.

Why?

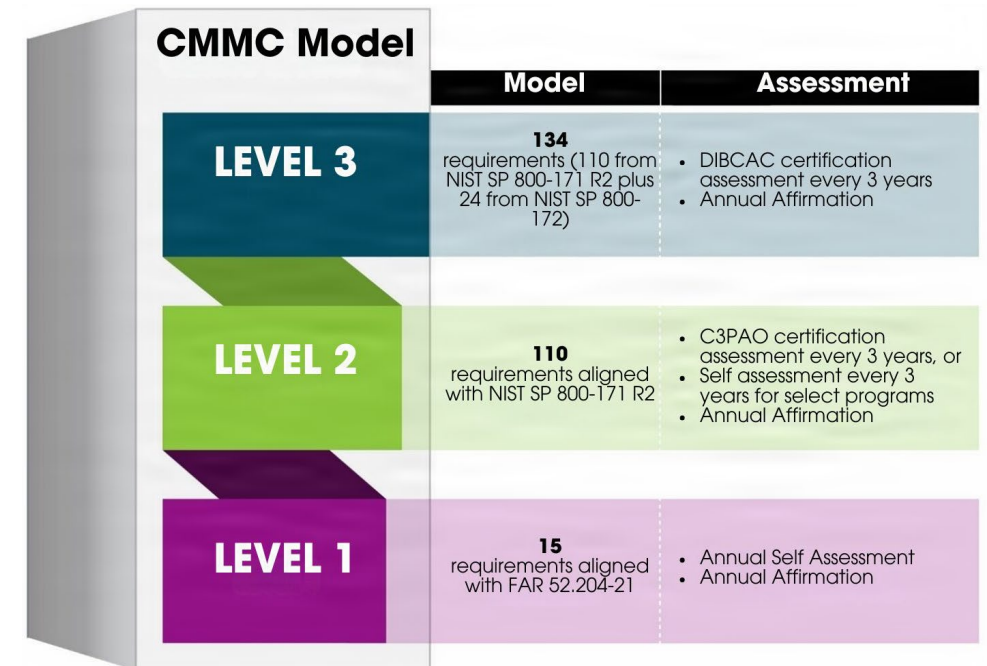
Protect the Defense Industrial Base (DIB) and DHA mission systems from cyber threats.

How?

Self-assessment or independent C3PAO/DIBCAC assessment prior to contract award or system operation (excluding COTS).

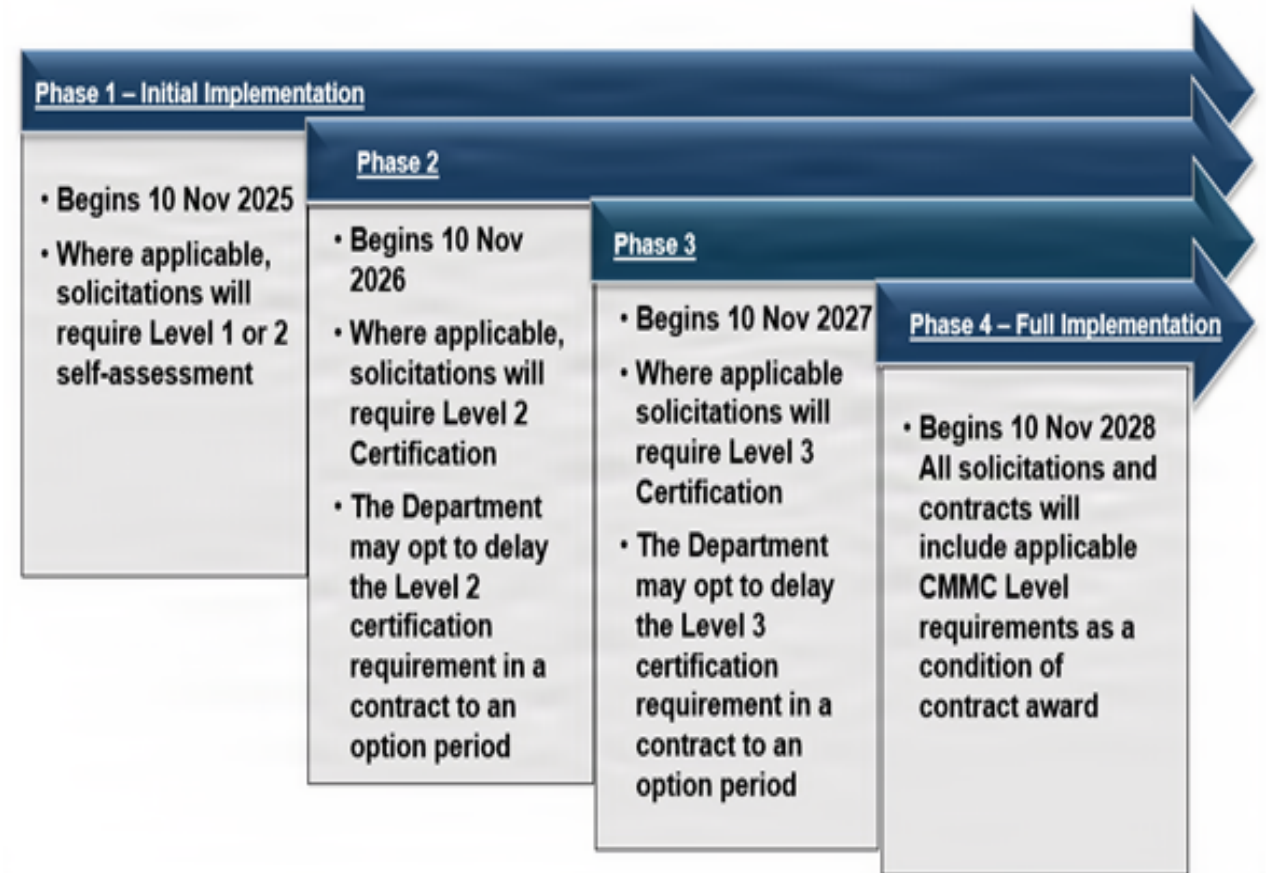
Alignment

Nests under DoW DIB Cybersecurity Strategy 2024, National Defense Strategy, and NIST Cybersecurity Framework.



CMMC Phases and Dates

- Phase 1 - Self Assessment (Level 1/2) only
- Phase 2 - Self-Assessment (1/2) + Level 2 (C3PAO)
- Phase 3 - Self-Assessment (1/2) + Level 2 (C3PAO) + Level 3 (DIBCAC)



CMMC – DHA Way Ahead

- IPT established documentation and process to capture all efforts requiring CMMC
- CMMC requirements to be inserted where appropriate into Contracts for all new and current contracts
- CMMC Mailbox is established for consultation: [dha.ncr.cio-j6.mbx.dha-cmmc-cell@health.mil](mailto:j6.mbx.dha-cmmc-cell@health.mil)
- Reach out to the above if there are any questions on applicability and level

2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM

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

Accelerated Delivery: Transforming Cybersecurity Approvals into Risk Intelligence

Achieving Faster, More Secure Outcomes Through Process Standardization and
Intelligent Automation



Phase 1: Building the Foundation for Speed

- **Document Current Workflows**
 - To eliminate ambiguity and create a single source of truth for the approval lifecycle.
- **Complete Workflow Documentation**
 - Achieve full completion of package lifecycle workflow documentation by end of September 2026.
- **Release Candidate Checklist**
 - To Standardize reviews, reduce reviewer work, and ensure high-quality submissions from the start.
- **Test and Finalize Checklist**
 - Test the universal checklist with real submissions and publish final version.

Mapping and Automating NIST 800-53 Controls for Efficient Validation

- **Hybrid Control Map Development**
 - Analyze NIST 800-53 controls to create a Hybrid Control Map distinguishing automated and manual validation methods.
- **Presumptive Crosswalk Completion**
 - Complete a full crosswalk of controls against tools categorized as automated, hybrid, or manual.
- **Feasibility Testing and Reclassification**
 - Test the crosswalk using real-world telemetry to reclassify controls accurately.
- **Documentation and Approval**
 - Compile all documentation for leadership review and obtain signed approval of the Hybrid Control Map.

Impact: This Hybrid Control Map is the blueprint for automation. By defining what can be machine-validated, we reduce manual review cycles and shift our experts' focus from paperwork to actual risk analysis.

The 80/20 Rule: Driving Efficiency in Approvals.

- **Goal: Achieve an 80% 'First-Pass Yield'**
 - 8 out of 10 packages are approved on the first submission.
 - No amendment needed (package is not sent back for corrections).
 - No variance allocation required (packages meet the standard without needing special exceptions)

Impact: This frees up our senior reviewers to focus on the 20% of complex, high-risk systems that truly require manual deep-dives, rather than chasing routine paperwork.

Conclusion

We are executing this in three deliberate phases: Standardizing our foundation, Deploying intelligent automation, and Scaling to achieve predictive risk management. A proactive, data-driven risk intelligent engine.

This it is not about faster approvals. It is about strengthening our security posture and making cybersecurity a true enabler of our DHA mission.

RME Panel Questions From The Audience



At this time, the Leadership Panel is open to questions from the audience

Contact Us

Mr. Richard Gasperoni
RME COO

 richard.gasperoni.civ@health.mil

Mr. Marc Shelton
RME Division Chief

 marc.d.shelton@health.mil

Ms. Maria Cante
RME Branch Chief

 maria.cante.civ@health.mil

Mr. David Lima
RME Branch Chief

 david.j.lima.civ@health.mil

LCDR Kerry Miller
RME Cybersecurity Lead

 kerry.n.miller2.mil@health.mil

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

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

Thank You!



UNCLASSIFIED