Logistics

- All attendees in "Listen Only Mode"

- Please ask content related questions in Q&A

- Recording, final slides, and resources shared within 24 hours

- Please take a few minutes to provide feedback via survey prompt at the end of this session

Introductions/ About Clearwater & Redspin

Dave Bailey, EMBA, CISSP | Moderator

VP, Consulting Services, Security at Clearwater

- 24 years in cybersecurity with 14 years focused on protecting the healthcare industry

- Served as Director of Technology and Security at Mary Washington Healthcare responsible for technology leadership and acted as designated HIPAA Security Official (2009 – 2016)

- Subject Matter Expert in cyber risk management, NIST Cybersecurity Framework assessment and implementation

- Experience in advising boards and senior leaders in cyber incidents, risk analysis, and strategy development

- Served 13 years in the United States Air Force, both on Active Duty and Reserves as a Communications and Information Officer with assignments at the Pentagon, Langley AFB, Eskan Village Saudi Arabia, and Peterson AFB.

Introductions/ About Christus Health, a USFHP

Dave Duclos, CISA, CISM, CISSP, CDPSE, CPHIMS | Panelist

Director and Deputy CISO, ITSEC/Cybersecurity at Christus Health

- Joined Christus Health in 2017 as System Director & Deputy CISO, leading SOC and SAC teams.

- Former Senior VP of IT and CISO in a multi-state hospital and emergency room company.

- Held various technical leadership roles in telecom, education, law enforcement, and the US Air Force over 25+ years.

- Holds bachelor's degrees in business management and computer & information science, an MBA, and several professional certifications (CISA, CISM, CISSP, CDPSE, CPHIMS).

- Active in professional organizations including FBI InfraGard, ISC2, ISACA, and HIMSS.

Introductions

Dr. Thomas Graham | Panelist

VP, CISO at Redspin

- 15+ years of Cybersecurity Leadership in the Commercial Healthcare and Government space
- 6 years leading the Mitigation and Remediation group for the Defense Health Agency (DHA)
- 4 years as an Information Security officer for MARCORSYSCOM and the Defense Information Security Agency (DISA)
- Current Chair – Management Information Systems (MIS) Advisory Board at East Carolina University (ECU), Prior member of HIMSS Security and Privacy Committee, Member AFCEA and HIMSS
- FedHealth IT Award for Innovation winner
- Ph.D. in Information Technology, MS in Technology Systems, and MBA
- Certified CMMC Assessor (CCA) and Provisional Instructor (PI)
- Architect of the first CMMC Authorized C3PAO

5

Introductions

Robert Teague | Panelist

Director, CMMC Services, at Redspin

- 30+ years of experience in information technology and cyber security operations in the United States Army

- 5+ years providing consultation and management to the defense industrial base (DIB), health care systems, and their supporting businesses

- Cybersecurity Maturity Model Certification (CMMC) Certified Assessor (CCA) and Certified Professional (CCP)

- Member of the Exam Development Committee, developing and validating the certification examination for the Cybersecurity Assessor and Instructor Certification Organization (CAICO)

- Member of the CMMC Standards Council

- BA in Business Administration; MBA Business Administration and Strategic Leadership, Graduate of the United States Army Sergeants Major Academy, Class 62

Healthcare and the DoD Preparing for CMMC Compliance
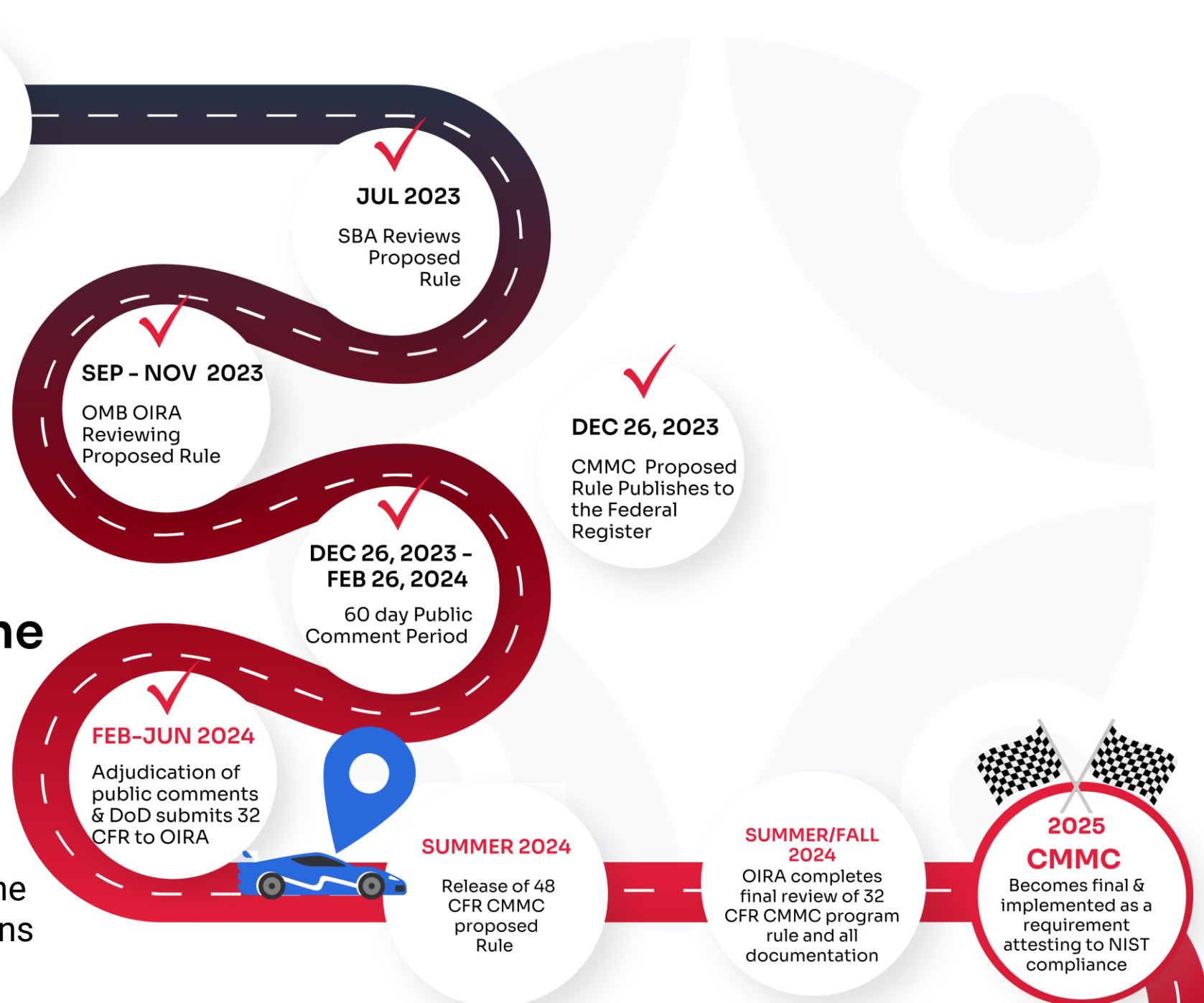
CMMC Background & Importance

- Explain why the Department of Defense established the CMMC program and its significance for healthcare organizations handling ePHI?

- What are the key differences between CMMC and other cybersecurity frameworks that healthcare organizations might already be familiar with?

Rulemaking Process and Compliance Timelines:

- Provide an overview of the current status of the CMMC rulemaking process and what we can expect in the coming months?
  - What are the key compliance timelines that healthcare organizations need to be aware of regarding CMMC certification?

CMMC 32 CFR Rulemaking Process and EstimatedTimeline Projections

*32 CFR for CMMC is the federal regulation that encompasses the **rules and guidelines for implementing the CMMC** within the Department of Defense's operations and activities.

NOV 2021
DoD Published Notice of Proposed Rulemaking

JUN 2023
DoD Drafted Proposed Rule

JUL 2023
SBA Reviews Proposed Rule

SEP – NOV 2023
OMB OIRA Reviewing Proposed Rule

DEC 26, 2023
CMMC Proposed Rule Publishes to the Federal Register

DEC 26, 2023 – FEB 26, 2024
60 day Public Comment Period

FEB-JUN 2024
Adjudication of public comments & DoD submits 32 CFR to OIRA

SUMMER 2024
Release of 48 CFR CMMC proposed Rule

SUMMER/FALL 2024
OIRA completes final review of 32 CFR CMMC program rule and all documentation

2025 CMMC
Becomes final & implemented as a requirement attesting to NIST compliance

CMMC 48 CFR Rulemaking Process and Estimated Timeline Projections

DEC 2023
DoD initial announcement of intention to establish a CMMC contract clause.

MAR 2024
Draft Rule Public Comment Period

APR-JUN 2024
DoD reviews and analyzes public comments.

JUL 2024
Integration of feedback. Revised draft rule based on public comments.

AUG-SEP 2024
OIRA OMB reviews the revised draft.

OCT-NOV 2024
Final rule published in the Federal Register. Official & implementation of the CMMC contract clause.

2024-2025 CMMC
DoD begins enforcement of the new CMMC requirements in contracts.

*48 CFR for CMMC is the federal regulation that integrates CMMC requirements into defense contracts.

Determining the Need for Certification & Getting Started

- How can a healthcare organization determine if they need CMMC certification?

- What are the first steps a healthcare organization should take when beginning their journey towards CMMC compliance?

- Can you share any tools or resources that can help organizations kickstart their CMMC implementation process?

Clearwater | Redspin. A Division of Clearwater | CHRISTUS Health.

CMMC in Healthcare: Best Practices and Challenges

- Case Study: Christus Health
  - The Need for CMMC
  - Preexisting NIST compliance
  - What is your current level of maturity?
  - Lessons learned
- What are some commonly missed opportunities/oversights in CMMC that healthcare organizations should pay special attention to?
- How can organizations balance the need for stringent CMMC requirements with the practical realities of their operational environments?

Future outlook

- Once an organization achieves CMMC certification, what are the best practices for maintaining compliance over the long term?

- How can organizations stay updated with any changes or updates to the CMMC requirements?

- How do you foresee the implementation of CMMC impacting the broader healthcare industry, particularly in terms of cybersecurity posture and partnerships with the DoD?

Audience Q&A

Dave Bailey

Dave Duclos

Dr. Thomas Graham

Robert Teague

Upcoming Events & Resources

Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

Thursday, August 1

[Register here](#)

OCR-Quality® Risk Analysis Working Lab 2024: Beginning August 7th @ 11:00 am CT

[Register here](#)

Redspin - CMMC Connect Thursday, August 29 @ 12:00 pm CST

[Register here](#)

Making the Move to Proactive Patient Privacy Monitoring | September 10 @ 12:00 CST

[Register here](#)

Clearwater

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Redspin
A Division of Clearwater

www.Redspin.com

888. 907. 3335

info@Redspin.com

linkedin.com/company/redspin-inc

Clearwater

www.clearwatersecurity.com

800. 704. 3394

linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.