Emerging Cybersecurity Trends

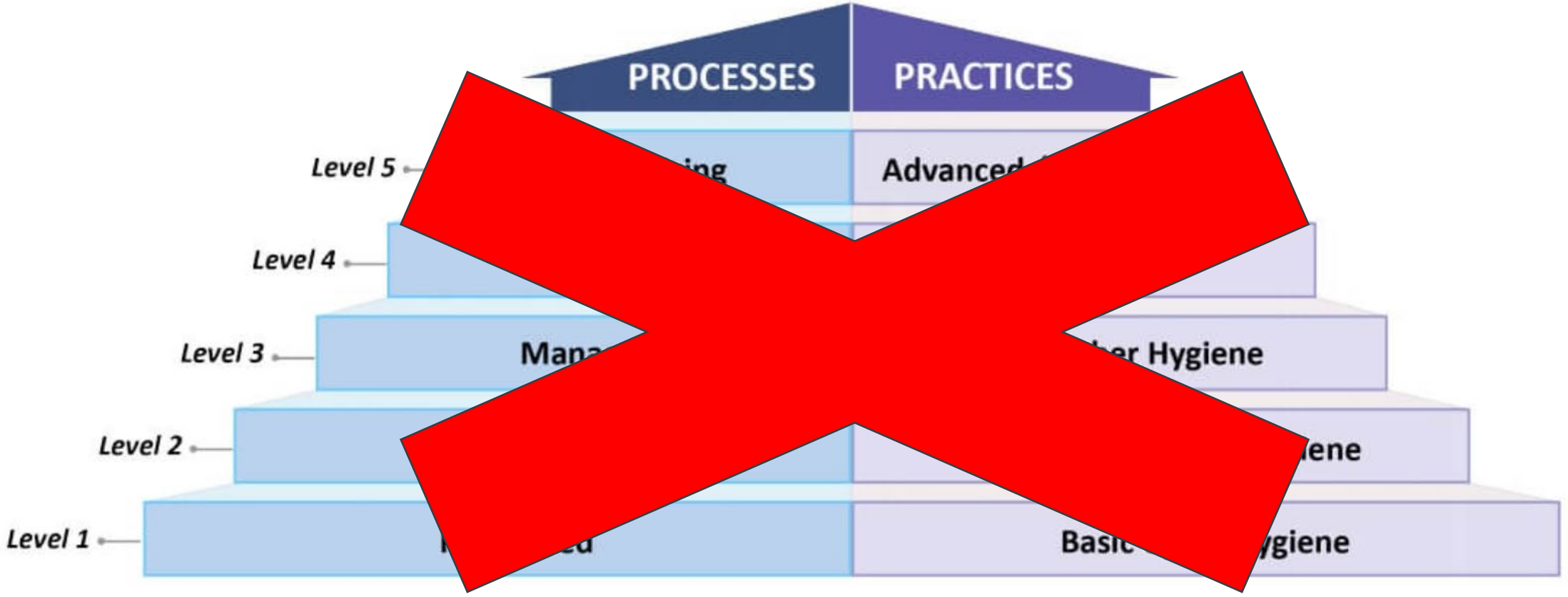
Michael Montalbano

BLANKROME

Cybersecurity Maturity Model Certification (CMMC)

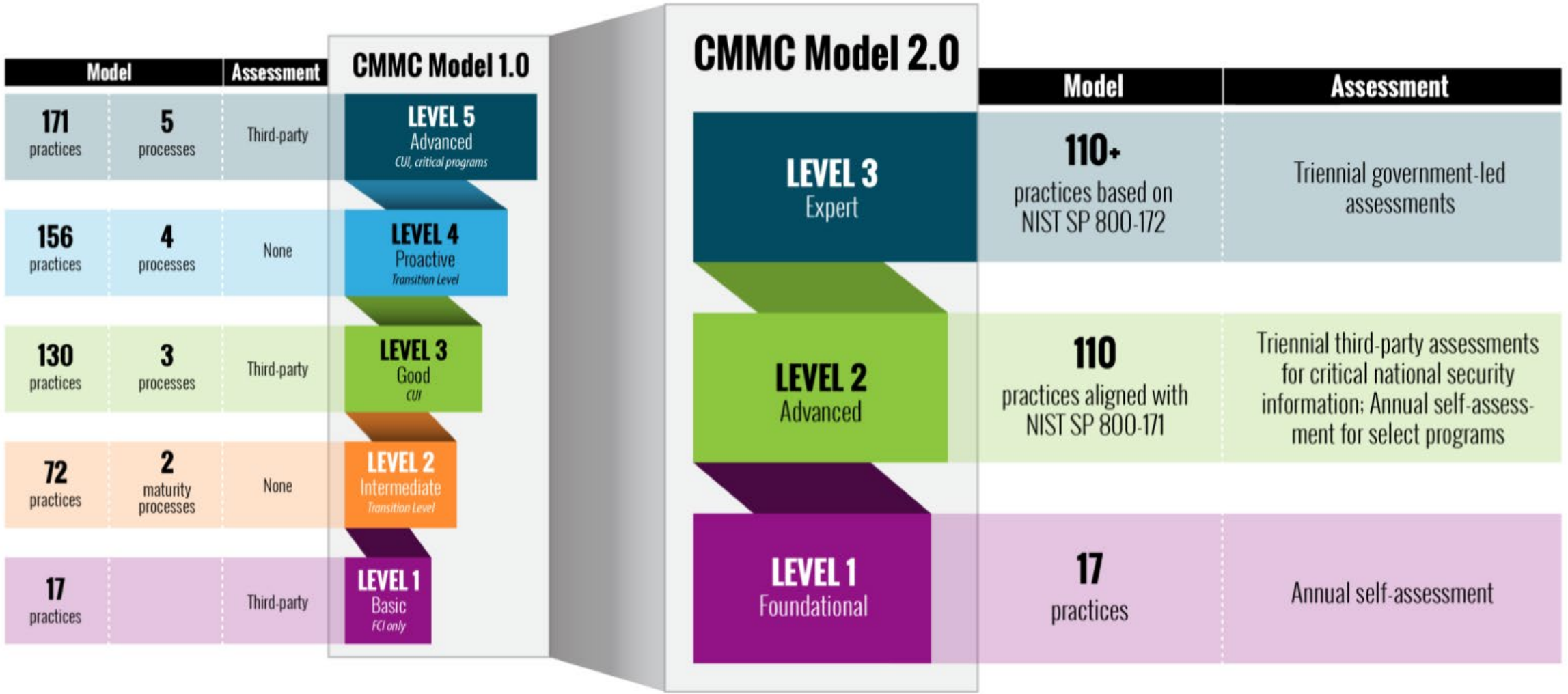
BLANKROME

CMMC 1.0



BLANKROME

CMMC 2.0



CMMC 2.0 – Plan of Action and Milestones ("POA&M")

- CMMC 1.0 required a contractor to meet every practice and process.
- CMMC 2.0 now allows contractors to submit a POA&M for those cyber practices and processes that it does not yet meet.
- If contractor can show that it is working towards meeting all of the requirements of its CMMC 2.0 level, it should still be permitted to continue work on the DOD acquisition.
- DOD has also signaled that it will waive CMMC requirements, if necessary.

BLANKROME

CMMC 2.0 – Increased Risk of False Claims Act Liability

- Under CMMC 1.0, contractors could rely on third-party certification
- Most contractors will now submit self-assessments
- Assessment standards can be vague and ambiguous
- Increased scrutiny from the Department of Justice
- Third-party assessments could mitigate risks

BLANKROME

CMMC 2.0 – Who Needs To Comply?

- **DOD Prime Contractors**
  - Major exception: COTS suppliers
  - Awaiting acquisition threshold
- **DOD Subcontractors**
  - Federal Government defines subcontractor broadly
  - Self-assessment will greatly reduce compliance burdens
  - Control of information flow can further reduce compliance burdens

BLANKROME

CMMC 2.0 – Timeline

- DOD has suspended CMMC 1.0.
- DOD will not require contractors to comply with CMMC requirements until new CMMC 2.0 rules are published.
- DOD is not expected to publish new rules until at least summer 2022, but more realistically not until 2023.
- DOD has not stated whether CMMC 2.0 immediately will go into effect.

BLANKROME

CMMC 2.0 – Takeaways

- Determine appropriate CMMC level
- Determine how information will be stored and accessed
- Start putting practices and policies in place now
- Prepare your subcontractors (but remember there is flexibility)

BLANKROME

President Biden's EO on Improving the Nation's Cybersecurity

- Signed by President Biden on May 12, 2021
- Follows High-Profile Cyberattacks
  - Colonial Pipeline
  - SolarWinds
  - Office of Personnel Management/MS Exchange
- Big Impact on Contractors

BLANKROME

What Does the EO Cover?

- Cyber Incident Reporting and Detection Requirements
- Modernized Cybersecurity Standards
- Software Security Requirements
- Cybersecurity Safety Review Board (and Event Log)
- “Playbook” for Cyber Incident Responses

BLANKROME

Practical Takeaways

- Civilian Agency Contractors Will Need To Catch Up
- Expanded Incident Response Requirements
- Uniform Requirements Could Ease Regulatory Burden
- Outstanding Questions Around Immunity and Proprietary Information

BLANKROME