APEX ACCELERATORS

OHIO UNIVERSITY | Voinovich School of Leadership and Public Service

Ohio University Apex Accelerator

What is Cybersecurity? Why is It Critical for Your Business?

What we are covering?

- Cyber Hygiene
- Current standards
- Upcoming Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) Level I & II readiness recommendations
- OU’s CMMC Readiness Program

Cyber Hygiene

"Cyber hygiene is a reference to the practices and steps that ***users*** *of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted." (*[*Digital Guardian*]*)*

Why Cyber Hygiene?

- Necessary in all types of industries including
  - Medical
  - Financial
  - Auto
  - Energy & Utilities
  - Government
- The risk of lax Cyber Hygiene is COSTLY:
  - Recent studies have shown that the average cost of a data breach to small business can range from $120,000 to $1.24 million, and that's strictly limited to a small business market (March '23) (Business.com)
  - IP Costs, Downtime, Lost Customer Base, Outright Ransom
- Can be a great differentiator for your business

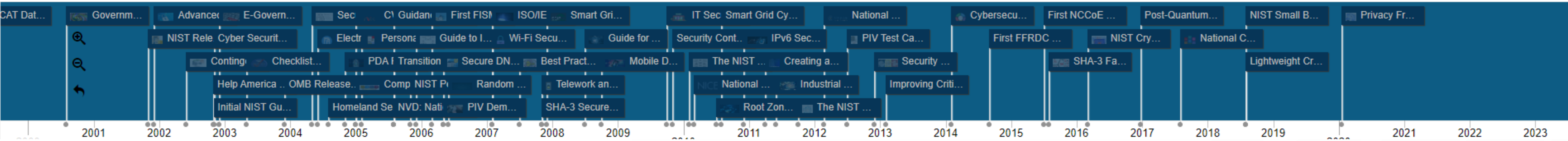
Current Standard

- NIST 800-171
  - CUI established by EO 13556 in 2010
  - Federal Information Security Modernization Act (FISMA) in 2014
    - Enacted after several security breaches
  - Followed by NIST 800-53 & NIST 800-171
- Required for:
  - DoD
  - GSA
  - NASA
  - University and Research Institutes Supported by Federal Grants
  - DIBBS Access
  - And more……

Current Standard

- NIST 800-171 Controls
  - Access controls
  - Awareness and training
  - Audit and accountability
  - Configuration management
  - Identification and authentication
  - Incident response
  - Maintenance
  - Media protection
  - Physical protection
  - Personnel security
  - Risk assessment
  - Security assessment
  - System and communications protection
  - System and information integrity

Timeline and Current NIST



- DFARS 252.204-7019 - Notice of NISTSP 800-171 DoD Assessment Requirements
  - (1) The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) () for all covered contractor information systems relevant to the offer.
  - (2) If the Offeror does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the Offeror may conduct and submit a Basic Assessment to for posting to SPRS in the format identified in paragraph (d) of this provision.
- DFARS 252.204-7020 - NIST SP 800-171DoD Assessment Requirements (Basic Assessment)
  - (1) Is based on the Contractor’s review of their system security plan(s) associated with covered contractor information system(s);
  - (2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and
  - (3) Results in a confidence level of “Low” in the resulting score, because it is a self-generated score

Safeguarding Covered Defense Information and Cyber Incident Reporting

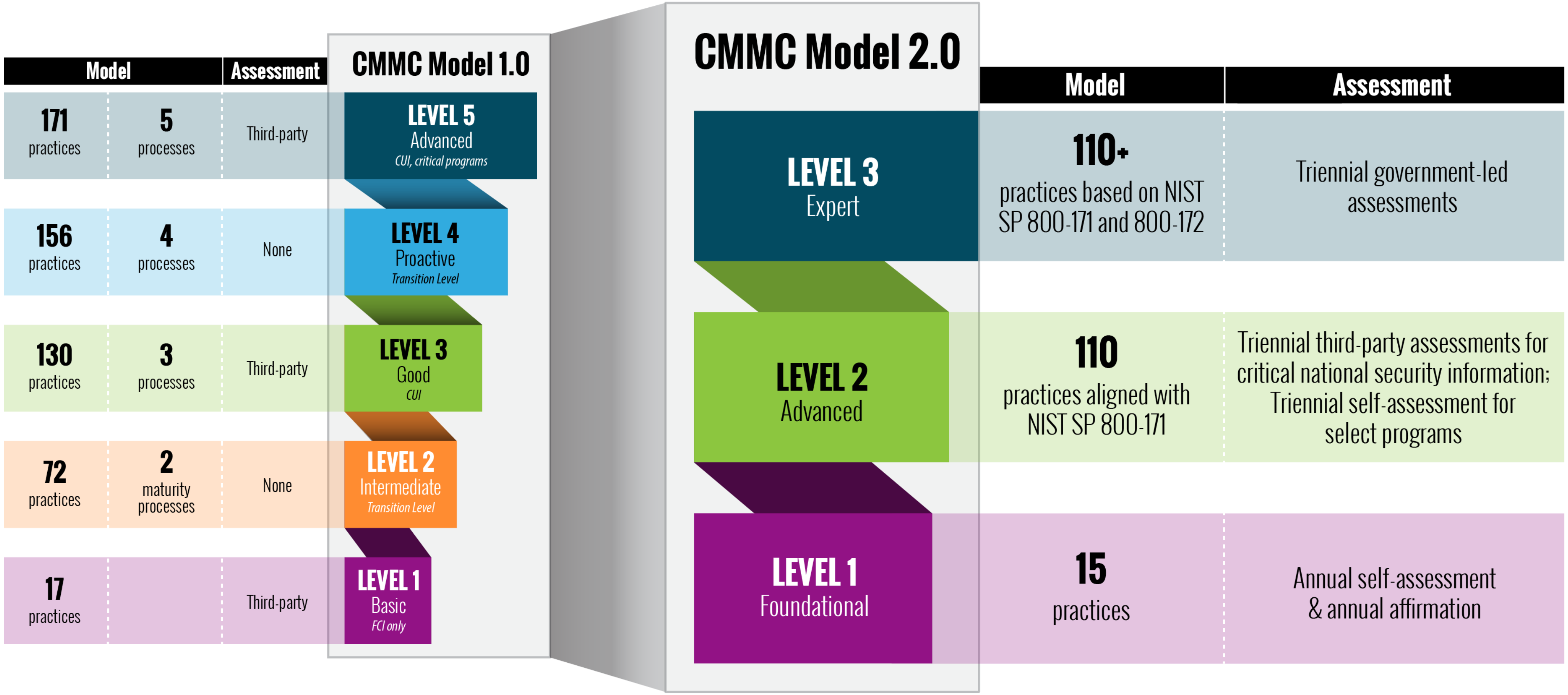
- DFAR 252.204-7012
  - 1) Safeguard covered defense information
  - 2) Report cyber incidents
  - 3) Submit malicious software
  - 4) Facilitate damage assessment
- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- Verify and control/limit connections to and use of external information systems.
- Control information posted or processed on publicly accessible information systems.
- Identify information system users, processes acting on behalf of users, or devices.
- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- Identify, report, and correct information and information system flaws in a timely manner.
- Provide protection from malicious code at appropriate locations within organizational information systems.
- Update malicious code protection mechanisms when new releases are available.
- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed

CMMC

In November 2021, the Department announced “CMMC 2.0,” an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Enforce DIB cybersecurity standards to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Perpetuate a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

What's Next? CMMC 2.0



CMMC Model 1.0

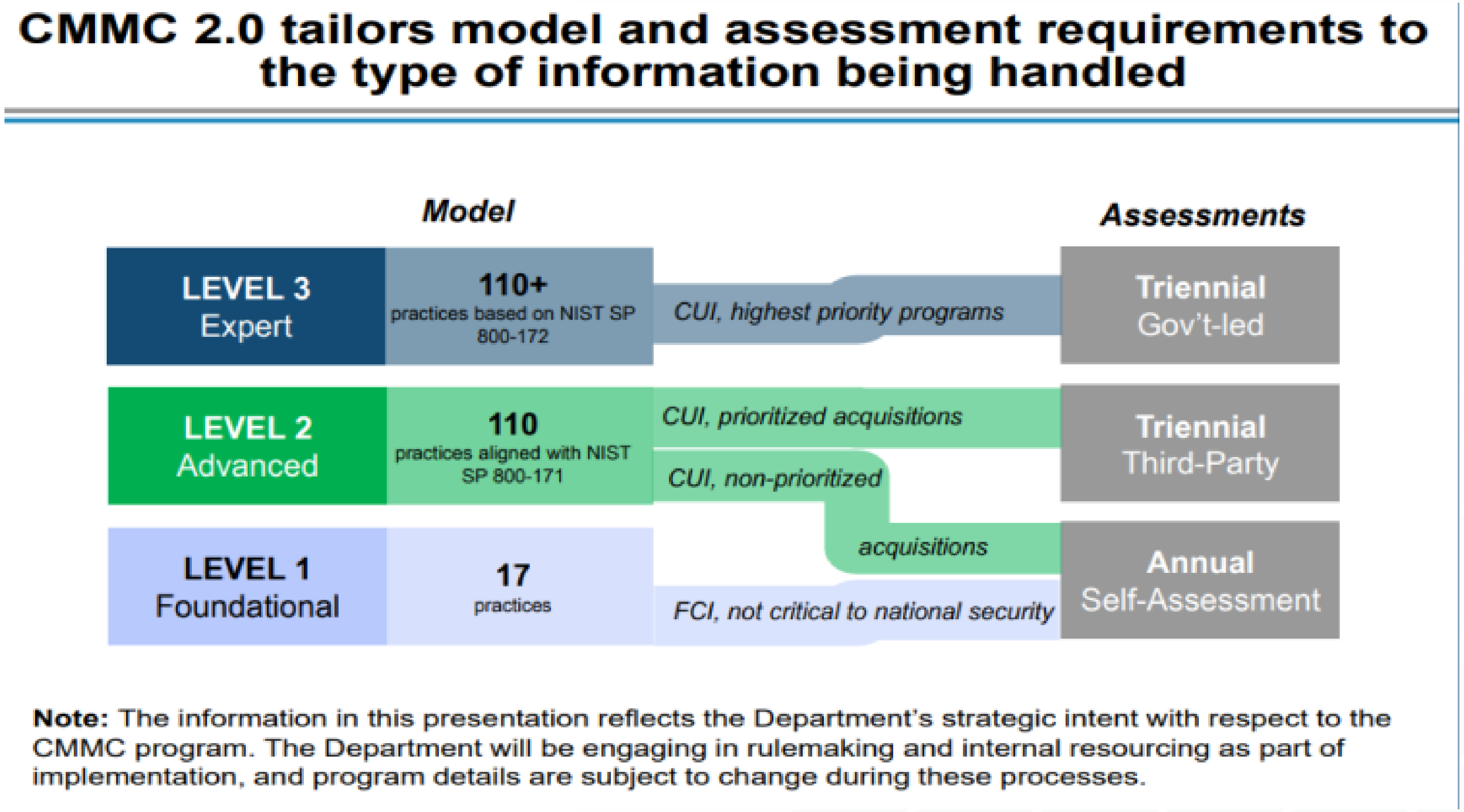
Model		Assessment	CMMC Model 1.0
171 practices	**5** processes	Third-party	**LEVEL 5** Advanced *CUI, critical programs*
156 practices	**4** processes	None	**LEVEL 4** Proactive *Transition Level*
130 practices	**3** processes	Third-party	**LEVEL 3** Good *CUI*
72 practices	**2** maturity processes	None	**LEVEL 2** Intermediate *Transition Level*
17 practices		Third-party	**LEVEL 1** Basic *FCI only*

CMMC Model 2.0

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	**110+** practices based on NIST SP 800-171 and 800-172	Triennial government-led assessments
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Triennial self-assessment for select programs
LEVEL 1 Foundational	**15** practices	Annual self-assessment & annual affirmation

**** Comparison between CMMC Models 1.0 and the planned CMMC Model 2.0. The CMMC Model 2.0 is notional until rulemaking is completed. ****

What's Next? CMMC 2.0



CMMC 2.0 tailors model and assessment requirements to the type of information being handled

Model			Assessments
LEVEL 3 Expert	**110+** practices based on NIST SP 800-172	*CUI, highest priority programs*	**Triennial** Gov't-led
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	*CUI, prioritized acquisitions*	**Triennial** Third-Party
		CUI, non-prioritized acquisitions	**Annual** Self-Assessment
LEVEL 1 Foundational	**17** practices	*FCI, not critical to national security*	**Annual** Self-Assessment

Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

OU CMMC Program

APEX clients can take advantage of free cybersecurity counseling to prepare for the future CMMC 2.0 regulations. Requirements for the program:

- Client is an Ohio-based business.
- Client is or wants to be part of the Defense Industrial Base.
- Client must register with their local SBDC.
- Client must be referred by their APEX counselor.

- Eligible APEX clients may receive up to 15 hours of consulting provided by a cybersecurity consultant. This counseling will assist clients in preparing for Level 1 certification under the CMMC 2.0 model. Client expected to certify under Level 2 may receive additional free counseling. This counseling will also help clients understand current Defense Federal Acquisition Regulation Supplement (DFARS)cybersecurity requirements of defense contractors.

Our Consultants

S|C SECURANCE CONSULTING

Our Consultants

ANTHONY TIMBERS

PROTECT YOUR COMPANY WITH A CYBERSECURITY PLAN

Additional Resources

- Ohio MEP Network
- Blue Cyber
- Project Spectrum
- Cyber AB

APEX ACCELERATORS

Ohio Apex Accelerator at Ohio University

Billy Grill

bgrill@ohio.edu

OHIO UNIVERSITY | Voinovich School of Leadership and Public Service