RESPONSE TO REPORT DODIG-2025-056 PURSUANT TO THE JAMES M. INHOFE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2023, PUB. L. NO. 117-263, SECTION 5274

The Department of Defense Office of Inspector General (DoD OIG) attaches the following response received from specifically identified non-governmental organization or business entity as required by the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Public Law No. 117-263 § 5274.

The DoD OIG offers no comment and makes no representations, express or implied, of any nature with respect to the matters stated in the attached response.

12 February 2025

From: Matthew Travis
Chief Executive Officer

To: Office of the Inspector General, U.S. Department of Defense

Subj: Response to Audit Report on Authorization of C3PAOs in the CMMC Program

Ref: (a) Report No. DODIG-2025-056, "Audit of the DoD's Process for Authorizing Third-Party Assessment Organizations to Perform Cybersecurity Maturity Model Certification 2.0 Assessments," January 10, 2025

1. From August 2023 through October 2024, The Cyber AB and its subsidiary, the Cybersecurity Assessor and Instructor Certification Organization (the "CAICO"), participated in the Department of Defense Office of the Inspector General (DoD OIG) Audit of the Authorization process for CMMC Third-Party Assessment Organizations (C3PAOs), providing full cooperation through responses to requests for information, submission of data and archival records, and taking part in multiple rounds of interviews with the OIG Audit team.
2. The Cyber AB and the CAICO recognize and appreciate the dedicated effort, unwavering professionalism, and considerate and engaging approach of the DoD OIG Audit team throughout the entire project. Although we disagree with the Audit team's interpretation of what we were—and were not—authorizing on a preliminary basis during CMMC's protracted rulemaking period, as described below, this disagreement does not detract from our high regard for the conduct of the Audit team, nor from its identification of areas where The Cyber AB's quality assurance rigor should be improved.
3. Pursuant to Section 5274 of Public Law 117-263, non-governmental organizations and business entities have the opportunity to respond to OIG reports in which they are mentioned.
4. This memorandum constitutes the formal response of both The Cyber AB and the CAICO to the following findings and comments contained in reference (a):
   a. Page 1, "Objective": *"The objective of this audit was to determine whether the DoD ensured that the process for authorizing third-party organizations to perform Cybersecurity Maturity Model Certification (CMMC) 2.0 assessments was effectively implemented."*
      - **Response:** The premise of the audit itself was unrealized and unsubstantiated as The Cyber AB had not yet implemented a process for authorizing C3PAOs to perform CMMC assessments at the time the Audit commenced through to its completion. The Cyber AB did not authorize <u>any</u> C3PAOs to perform CMMC assessments during the entirety of the audit period. Authorization of C3PAOs to conduct CMMC Level 2 certification assessments did not commence until 2 January 2025, following the commencement of the CMMC Program as codified by the 32 CFR part 170 final rule, which entered into force on 16 December

2024. Prior to that, during the entirety of the three-year CMMC federal rulemaking process, The Cyber AB had administered a non-CMMC binding, preliminary authorization program for C3PAO candidates in order to accomplish the following: 1) facilitate capacity-building during rulemaking so that there would still be a C3PAO cadre in existence ready for actual CMMC Authorization upon completion of the 32 CFR part 170 final rule; 2) recognize the accomplishments of those C3PAO candidates that had successfully passed the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessment of NIST SP 800-171 Rev. 2 security requirements and that had also met the other *preliminary and anticipated* C3PAO requirements; and 3) provide an opportunity for these C3PAO companies to remain economically viable during the protracted rulemaking process by issuing an "authorized" credential that would enable them to gain valuable practical assessment experience by participating in the DIBCAC Joint Surveillance Voluntary Assessment (JSVA) initiative, as well as use their C3PAO status to provide mock assessments to companies within the Defense Industrial Base (DIB) preparing for CMMC. Upon reflection, we made a mistake in utilizing the term "authorization" to convey this preliminary status upon this group of C3PAOs, which ultimately confused the issue as to what C3PAO authorization really meant. That notwithstanding, at no time were any of these C3PAOs authorized to conduct CMMC assessments. In fact, the letter that I issued to these C3PAOs specifically and explicitly stated that they were "not yet authorized to conduct CMMC assessments." Moreover, upon publication of the 32 CFR part 170 Proposed Rule in December 2023, the C3PAO cadre was repeatedly informed that they would all need to complete successfully the formal C3PAO authorization process as informed by the eventual publication of the CMMC 32 CFR part 170 Final Rule. It was always known to the C3PAO cadre that the authorization status conveyed to them during the preliminary rulemaking period would be invalidated upon commencement of the formal CMMC Program as codified by the 32 CFR part 170 Final Rule entering into force.

b. Page 5, "The candidate C3PAOs must successfully complete a series of 12 requirements before they can be authorized to perform the CMMC Level 2 assessments."

   - **Response:** This statement is a vestige of the CMMC 1.0 program that was obviated by the CMMC 2.0 rulemaking process. C3PAOs must meet 21 discrete requirements to obtain Authorization. The Cyber AB never authorized C3PAOs for CMMC certification assessments under these old requirements, but we were remiss by not removing this language from our public-facing website once rulemaking commenced. In some cases, the Audit team held us accountable for language that was on our website instead of the requirements that were or were not included in our no-cost contract with the Department or that eventually appeared in the 32 CFR part 170 Final Rule.

c. Page 10, "Cyber AB officials ensured that the candidate C3PAOs met 10 of the 12 requirements before authorizing them to perform CMMC Level 2 assessments."

   - **Response:** The Cyber AB did not authorize any C3PAOs to perform CMMC Level 2 assessments during the Audit period, nor under these outdated requirements.

d. Page 10, "Cyber AB officials did not maintain a signed C3PAO Agreement and Code of Professional Conduct for 2 of the 11 C3PAOs that we reviewed," leading to the finding that the Cyber AB "cannot enforce termination of the C3PAO's authorization to perform CMMC Level 2 assessments based upon a breach or violation."

- **Response:** The interim C3PAO Agreement that companies initially signed with The Cyber AB when they applied to the C3PAO program had a one-year termination clause contained therein, anticipating and providing for a new agreement that would be put in place following the completion of CMMC rulemaking, at which time formal C3PAO requirements would be codified. Admittedly, we were unable to locate 2 of the 11 requested interim and expired agreements as they were lost during our transition to a new data platform in 2022. But since The Cyber AB never authorized these companies to conduct CMMC Level 2 certification assessments, the obsolescence and absence of these agreements did not preclude us from enforcing termination of an authorization to conduct CMMC assessments that had never been granted.

e. Page 11, "Cyber AB officials did not verify that the QCLs for 4 of the 11 C3PAOs were certified."

- **Response:** The requirement for a formal quality control position within a C3PAO was not included in our original contract with the Department and evolved over time. At various points, this envisioned role had been informally called "quality control personnel (QCP)," "quality assurance individual," "quality control lead (QCL)," and others. Similarly, our understanding of the requirements for this eventual position also varied as CMMC rulemaking proceeded for over three years. Since we were unable to communicate with the CMMC PMO during rulemaking about the impending requirements for the CMMC Program, including for this position, our verification of the anticipated role was inconsistent.

f. Page 12, "Cyber AB Officials' Methodology for Verifying that CCAs and Certified QCLs Were on Staff Was Inadequate," citing a rationale of "Requesting a business email address is not an adequate method for verifying employment because if the candidate C3PAO's system administrators do not delete a user's email address when they leave the company, the user would still have an active email address. In addition, ensuring that the employee has a valid user email address does not provide verification that the employee is in a position responsible for leading and overseeing CMMC Level 2 assessments."

- **Response:** The Audit Team is correct in reporting that The Cyber AB often relied on the existence of a corporate email address as evidence that the Certified CMMC Assessor (CCA) had an employment or contractual agreement with the candidate C3PAO. The requirement itself is simply to ensure that the candidate C3PAO has the minimum threshold of certified personnel on their active roster to conduct a CMMC Level 2 certification assessment—there is no DoD requirement that a CCA must be a "W-2" employee with the C3PAO. We accept the inferred argument from the Audit team that there are more rigorous forms of evidence than an email address to determine if a C3PAO has agreements in place with a CCA, and we have since adjusted our process accordingly. Nonetheless, the logic that a CCA could still have a valid email address if the C3PAO system administrator does not delete the user's email account is not dissimilar from the logic that a copy of an employment agreement from a C3PAO human resource director documenting that a CCA is employed by the company only provides assurance that the CCA was employed on the day that the employment agreement was signed; the CCA could have been terminated by the C3PAO during the preceding week, month, etc. Ultimately, candidate C3PAOs are attesting to The Cyber AB during the Authorization Meeting that they have the minimal personnel onboard to conduct a CMMC Level 2 certification assessment, and they do so under the requirements to provide accurate and truthful information to The Cyber AB

pursuant to the CMMC Code of Professional Conduct (CoPC) and under the requirements to have qualified personnel under ISO/IEC 17020:2012, "Conformity assessment — Requirements for the operation of various types of bodies performing inspection". Moreover, the Audit finding that the email address does not provide verification that the CCA "is in a position responsible for leading and overseeing CMMC Level 2 assessments" is true but misguided. The verification method we utilize for confirming responsibility and competency comes from the CCA certification records provided by the CAICO, not the email address. When the candidate C3PAO requesting Authorization provides the names of their certified personnel, The Cyber AB confers with the CAICO to verify certification of those individuals. Only then does The Cyber AB request evidence of employment or contractual agreement between the C3PAO and the CCAs.

5. We understand that unequivocal trust and confidence in the CMMC Program by the DIB and the public is paramount for its success. This success can only be attained if the CMMC accreditation body—presently The Cyber AB—operates at the highest levels of competency, maturity, impartiality, and transparency. We welcome the recommendations of the Audit team in improving the quality assurance aspects of our processes and will work diligently with the CMMC Program Office to improve our operations accordingly.

Matthew Travis
Chief Executive Officer