U.S. Citizenship and Immigration Services

Non-Precedent Decision of the Administrative Appeals Office

In Re: 33966587

Date: SEPT. 27, 2024

Appeal of Texas Service Center Decision

Form I-140, Immigrant Petition for Alien Workers (National Interest Waiver)

The Petitioner,[1] a cyber security specialist, seeks employment-based second preference (EB-2) immigrant classification as a member of the professions holding an advanced degree, as well as a national interest waiver of the job offer requirement attached to this classification. *See* Immigration and Nationality Act (the Act) section 203(b)(2), 8 U.S.C. § 1153(b)(2).

The Director of the Texas Service Center denied the petition, concluding the record did not establish that a waiver of the required job offer, and thus of the labor certification, would be in the national interest. The matter is now before us on appeal pursuant to 8 C.F.R. § 103.3.

The Petitioner bears the burden of proof to demonstrate eligibility by a preponderance of the evidence. *Matter of Chawathe*, 25 I&N Dec. 369, 375-76 (AAO 2010). We review the questions in this matter de novo. *Matter of Christo's, Inc.*, 26 I&N Dec. 537, 537 n.2 (AAO 2015). Upon de novo review, we will dismiss the appeal.

On appeal, the Petitioner presents additional evidence and primarily reasserts his proposed endeavor's national importance under the first prong of *Matter of Dhanasar*, 26 I&N Dec. 884, 889 (AAO 2016). In particular, he argues that his artificial intelligence (AI) framework aligns with national security priorities and initiatives, and that it fosters U.S. economic competitiveness.

Upon review of the entire record, we adopt and affirm the Director's decision regarding the Petitioner's eligibility under *Dhanasar's* first prong. *See Matter of Burbano*, 20 I&N Dec. 872, 874 (BIA 1994); *see also Giday v. INS*, 113 F.3d 230, 234 (D.C. Cir. 1997) (noting that the practice of adopting and affirming the decision below has been "universally accepted by every other circuit that has squarely confronted the issue"); *Chen v. INS*, 87 F.3d 5, 8 (1st Cir. 1996) (joining eight circuit courts in holding that appellate adjudicators may adopt and affirm the decision below as long as they give "individualized consideration" to the case). We agree with the Director's well-reasoned decision that the Petitioner has not sufficiently demonstrated how his proposed endeavor would have a broader impact extending beyond his company and its clients, to rise to the level of national importance.

[1] The Petitioner has two alien registration numbers: [redacted] For best results, we encourage the Petitioner to use [redacted] when contacting the agency.

In his appellate brief, the Petitioner attempts to cure the deficiencies discussed in the Director's decision and argues that his endeavor is poised to combat cyberattacks through real-time threat detection and mitigation; enhanced national preparedness; and alignment with National Security Memorandum (NSM-22). The Petitioner also submits an updated letter from Dr. [redacted], a list of the Petitioner's prior work on various "Critical Infrastructure Sector" related projects, and other previously submitted evidence. While the Petitioner summarizes his proposed endeavor's noteworthy goals, his appellate submissions are, nevertheless, insufficient to overcome the Director's decision. The Petitioner has not adequately detailed in the record below, or on appeal, *how* he specifically plans to accomplish these goals and has not shown that his endeavor would have broader implications in the industry or U.S. economy.

Dr. [redacted] claims in her updated letter that the Petitioner's work has "significantly influenced" the cybersecurity industry, and will continue to do so in the future. However, she again does not provide specific examples or evidence demonstrating what these contributions were or how they affected the industry. Instead, she points to previously submitted documents "showcasing his accomplishments" and the newly submitted list of the Petitioner's projects. While she alleges that the Petitioner's "most cutting-edge work is protected by Non-Disclosure Agreements (NDAs) and/or is considered the Intellectual Property (IP) of the organizations he conducted the work for," she does not corroborate her assertions with any evidence. Additionally, contrary to her claim, the Petitioner's various white papers, without more, do not adequately show how his work "significantly influenced" the cybersecurity field particularly where, as here, the evidence does not reflect these papers were published, much less cited, by other experts in the field. Dr. [redacted] letter is insufficient to address the Director's concerns or otherwise resolve the deficiencies in the evidence.

Likewise, the Petitioner's list of "Critical Infrastructure Sector" related projects documents various activities the Petitioner reportedly performed in his career. Based on his own descriptions, however, the impact of his work appears limited to his company and its clients. The Petitioner has not explained how these activities demonstrate his work has had, or shows that his future work will have, broader implications in the cybersecurity industry.

The Petitioner also resubmitted a large number of documents already in the record. But, again, these documents do not demonstrate that the Petitioner's proposed endeavor will have broader implications. Most of these white papers provide only general information about the benefits of artificial intelligence and cybersecurity, and they do not elaborate on the Petitioner's proposed endeavor in sufficient detail, including *how* he plans to create and implement his framework. For example, the Petitioner states his framework will "[p]rocess large volumes of threat intelligence data from diverse sources . . . in real-time using Natural Language Processing (NLP)" and will "leverage[] anomaly detection techniques and real-time NLP which can analyze this data to identify unusual patterns potentially indicative of emerging cyberattacks." He generally references various pre-existing technologies he has "considered" using and states his framework will integrate NLP, anomaly detection, and predictive analytics. However, he does not articulate how he will knit these technologies and components together to build his "novel AI framework." While he vaguely describes stages of his "development and implementation plan," the evidence appears to indicate that his framework's composition is undefined and in flux. Although he asserts on appeal that *his* specific AI framework "positions the US at the forefront of cybersecurity," he does not articulate a specific design for his endeavor and, instead, seemingly intends build out a model based on the feedback of his potential clients.

The evidence submitted on appeal is not sufficient to overcome the Director's decision. Because the Petitioner did not establish his proposed endeavor's national importance as required by *Dhanasar's* first prong, he has not demonstrated eligibility for a national interest waiver. Further analysis of his eligibility under *Dhanasar's* second and third prongs, therefore, would serve no meaningful purpose, and we reserve those remaining issues and arguments. *See INS v. Bagamasbad*, 429 U.S. 24, 25 (1976) ("As a general rule courts and agencies are not required to make findings on issues the decision of which is unnecessary to the results they reach."); *see also Matter of D-L-S-*, 28 I&N Dec. 568, 577 n.10 (BIA 2022) (declining to reach alternative issues on appeal where an applicant is otherwise ineligible).

ORDER: The appeal is dismissed.