

Extreme Vetting For Visa Applicants

May 17, 2017

RELATED PRACTICES Immigration, International, Labor and Employment

On May 4, 2017, the Department of State (“DOS”) published in the Federal Register a Notice to implement the presidential initiative for extreme vetting of visa applicants. Emergency review of the DOS proposal has been requested from the Office of Management and Budget (“OMB”). The DOS has requested approval by May 18, 2017. If granted, the emergency approval would be valid for 180 days, although permanent approval could still be sought. The proposed screening protocols are significant because they are designed to mine considerably more data than current protocols.

U.S. Consulates are the visa-issuing authority and come under the purview of the DOS. The DOS’s proposal for enhanced data collection is undertaken to more “rigorously evaluate applicants for terrorism or other national security-related visa ineligibilities.” The DOS seeks to elicit additional information from applicants that pose a “threat profile.” Among the data the DOS desires to collect from this “subset of applicants” is:

- Travel history during the last fifteen years, including source of funding for travel;
- Employment history during the last fifteen years;
- Phone numbers and email addresses used during the last five years;
- Names and dates of birth for all siblings;
- Names and dates of births for all current and former spouses, or civil or domestic partners; and
- Social media platforms and identifiers, also known as handles, used during the last five years.

Some of the information is already collected on visa applications, but for shorter periods. But under the current proposal the DOS may also request detailed information (and supporting documentation) about travel history—if it appears to the consular officer that the applicant “has been in an area while the area was under the operational control of a terrorist organization.” Notably, the sibling data is a new application component, as is the request for social media identifiers and associated platforms. The DOS insists that failure to provide the requested information will not necessarily result in visa denial, provided the applicant has given a credible explanation.

The social media component is intended to be responsive to security threats supported and advanced through electronic means. The Public Notice, however, defines its boundaries, maintaining that consular officers will not request user passwords and will not attempt to subvert any privacy controls that applicants may have implemented on social media platforms. The restrictions walk back the desire by Department of Homeland Security Secretary John Kelly to also require passwords to evaluate internet activity.

What remains uncertain is what applicants or application profiles will trigger the enhanced screening. The DOS states that consular officers may opt for enhanced measures to “resolve an applicant’s identity” or to “vet for terrorism or other national security related visa ineligibilities” when the officer “determines that the circumstances of a visa applicant, a review of the visa application, or responses in a visa interview indicate a need for greater scrutiny.” No other guidance is provided in the Public Notice.

The foregoing measures may result in administrative delays. Clients can prepare for potentially longer wait times at U.S. Consulates abroad.