February 10, 2025

USCIS

Re: Support Letter for Dr. Kirill Nikitin's EB-1A petition

Dear USCIS Officer,

I am honored to support Dr. Kirill Nikitin's petition for classification as an Alien of Extraordinary Ability under the EB-1A category. Dr. Nikitin has made significant contributions to data privacy and computer security, advancing both theoretical foundations and practical applications. His exceptional expertise and innovative research firmly establish him as a leader in the field, while the nature of his work makes him an invaluable asset to the United States.

I offer this support as an internationally recognized expert in …

Given my expertise and service to the U.S. government, I believe that I am well-qualified to assess Dr. Nikitin's extraordinary ability and the national importance of his scientific contributions. While I am aware of Dr. Nikitin's contributions in several subfields of computer security and data privacy, I believe that his most outstanding achievements are in developing techniques for protection of metadata. Metadata come in many forms. What resources users access, who they communicate with, and how they do it constitute sensitive information that is often as important as the content of the communication itself. Dr. Nikitin's research focuses on protecting side information exposed during data encryption and protecting user access patterns—areas that are both technically challenging and vital to national security and individual privacy. As I testified to …, all data are personally identifiable information because even innocuous-looking data about an individual can be correlated with her identity. In an era where cyber threats and mass surveillance pose increasing risks, Dr. Nikitin's innovations contribute directly to the protection of U.S. infrastructure, businesses, and citizens from data exploitation.

I should clarify that Dr. Nikitin and I have never collaborated, and I know of him solely because of his research contributions. I, however, saw his in-person presentation at a research seminar at Purple Inc. offices because we invited him to present his work on protecting attributes of encrypted data, after it had just been adopted by Apple for use in iMessage. Dr. Nikitin's innovation in iMessage is a technique for obfuscating the length of encrypted data. Most encryption algorithms nowadays preserve the length of data when encrypting it. For example, the word "yes" would commonly be encrypted with three symbols, whereas the word "no" with two symbols. This is obviously a privacy issue in the messaging context because, even when encrypted, the two words would be easily distinguishable. Dr. Nikitin proposed a padding technique that struck the optimal balance between the size protection and the induced bandwidth overhead. Minimizing the overhead while providing the best possible protection is

critical, as a system like iMessage might be exchanging billions of messages every day. The fact that Dr. Nikitin's innovation provides this balance and that it is directly translated into deployment by a major technology company underscores the real-world impact of his work and its importance in securing communications at scale.

Dr. Nikitin's work on protecting user access patterns follows a long line of research on private information retrieval (PIR). PIR is a set of techniques for enabling a computer user to fetch an item from a database without revealing to the database which item it is. While PIR has been extensively studied in academic settings, all the prior approaches have been unsuitable for real-world deployment due to being insecure in the adversarial setting. Dr. Nikitin's work is the first to demonstrate how to make such protocols secure even when the database operator actively attempts to break the user's privacy. These security properties are crucial in applications requiring strong guarantees, such as secure cloud storage and privacy-preserving search. Dr. Nikitin's contributions bring the PIR technology significantly closer to practical deployment, enabling robust privacy protections in real-world systems.

In summary, I wholeheartedly endorse Dr. Nikitin's EB-1A petition. His exceptional abilities, pioneering research, and tangible real-world impact make him an extraordinary asset to the United States. I am confident that his continued contributions will further enhance America's leadership in data privacy, computer security, and innovation. For these reasons, I urge you to favorably consider his application.

Yours faithfully,

FFF