January 30, 2025

Department of Homeland Security
USCIS

Re: Letter of Support for Dr. Kirill Nikitin's Immigration Petition

To Whom It May Concern:

I am pleased to write this letter to express my full support for the immigrant petition submitted by Dr. Kirill Nikitin. Having closely worked with him, I can confirm that Dr. Nikitin is a scientist of outstanding talent, who has made contributions of major impact to our research field and whose expertise is of national importance to the United States.

Ny name is …

Dr. Nikitin is an established scientist in data and computer privacy. He has published multiple works in the most prestigious scientific venues, including the top-tier peer-reviewed conferences, such as the IEEE Symposium on Security and Privacy and the USENIX Security Symposium. These conferences are highly selective and attract groundbreaking research from leading experts in the field. The impact of Dr. Nikitin's work is reflected in its significant academic recognition—his publications have been cited more than 331 times by other researchers, which is an impressive number for a scientist at his career stage. This level of citation demonstrates that his contributions are not only relevant but also influential, shaping ongoing research and advancements in privacy enhancing technologies.

Dr. Nikitin's work on reducing metadata leakage from encrypted files and communication is one of his most influential contributions. Dr. Nikitin has studied the problem of encrypted-data formats exposing auxiliary information, such as the encryption suites used or the payload length. This kind of exposure can be exploited by traffic analysis, de-anonymization and website fingerprinting attacks and it has been extensively studied by the research community. Instead of sustaining the fragile balance and trying to distinguish which metadata were sensitive and could be exposed and which were not, Dr. Nikitin proposed a radical innovation of leaving no unencrypted metadata in ciphertexts whatsoever. While being ideal from the privacy perspective, this approach faced efficiency challenges due to requiring new ways of handling decryption, as a recipient would not know what algorithm or cryptographic key to use to decrypt a ciphertext without unencrypted markers. Dr. Nikitin's proposed decoding techniques enabled a recipient to

first efficiently find and decrypt the auxiliary markers and then to decrypt the data. This innovation has made it significantly more difficult for adversaries to perform traffic analysis or to infer sensitive information from encrypted data at-rest.

Dr. Nikitin's expertise in data privacy is of national significance to the United States. In recent years, the U.S. government has increasingly recognized the urgent need for advancements in privacy-preserving technologies, particularly in response to escalating cybersecurity threats. This has led to a rise in federally funded grant programs dedicated to this critical area. Dr. Nikitin contributed to a project funded by the Defense Advanced Research Projects Agency (DARPA), a government agency focused on developing cutting-edge technologies for national security. As part of this project, he devised techniques for metadata-private communication that made an individual's web activity to appear indistinguishable to a network observer, rendering it resistant to traffic analysis. By continuing his research in the United States, Dr. Nikitin will be well-positioned to further these vital efforts, advancing technologies that not only safeguard individual privacy but also strengthen national security and reinforce the country's leadership in technological innovation.

To conclude, Dr. Nikitin is a recognized leader in data and computer privacy research. If he is to stay in the United States, he will be a great asset to the country and will continue making important contributions in research and beyond. I, therefore, urge you to favorably consider his application for permanent residence in the United States.