January 20, 2025

Center Director
Department of Homeland Security
USCIS

Re: Independent Reference in Support of Dr. Kirill Nikitin's EB-1A Petition

Dear Immigration Officer:

I am pleased to write an independent reference letter on behalf of Dr. Kirill Nikitin in support of his Alien of Extraordinary Ability petition. Dr. Nikitin is one of a select few researchers who has risen to the very top of the field of computer security, specializing in software-update security, blockchains, and verifiable computation. Although we have never worked together personally or professionally, I am very familiar with Dr. Nikitin's work by way of his publications. I can confidently affirm his international reputation as an outstanding researcher and offer my full support of this petition.

My name is ...

Given my expertise, I can offer a good account of Dr. Nikitin's contributions to the field.

Dr. Nikitin is one of the world experts in security of software-update systems, a research area of national importance to the United States. As recent attacks, such as the breaches of government agencies through SolarWinds's software, have shown, software-update systems are a lucrative target for malicious actors because compromising a single access point can enable them to distribute malware to thousands of companies and users. Failures in the software-update process can also lead to the disruption of critical services. CrowdStrike-related outage, caused by a faulty software update, several months ago resulted in grounded flights, halted governmental services, and closed banks with the estimated worldwide financial damages of at least $10 billion. Hence, it is of paramount importance to design robust and secure mechanisms for the software supply chain.

As a response to this critical challenge, Dr. Nikitin developed an innovative framework, named CHAINIAC, that was the first to leverage decentralization and transparency to eliminate single points of failure and to enforce integrity in the software-release pipeline. At a high level, the framework secures each step of the software production process, from the development of the source code to the installation of the corresponding update on a user's device. Among other techniques, the framework introduced the concepts of collectively verified builds and skipchains. Prior artifact-verifiability approaches provided the guarantee

that a given source code could be deterministically compiled into some binary but did not establish any binding between the source code and the actual release delivered to user devices. CHAINIAC's innovation was to employ multiple servers that independently compiled a binary and then attested to a single valid release result that end users could trust. By leveraging skipchains, a novel data structure that Dr. Nikitin designed, CHAINIAC implemented a public release log that deflected targeted attacks on high-profile individuals. This work of Dr. Nikitin constituted a major contribution to the field and influenced the design of multiple follow-up architectures, including the Google's Binary Transparency project.

Another influential work by Dr. Nikitin that I am closely familiar with showed how to improve the performance of Replicated State Machines (RSMs) by utilizing outsourced verifiable computation. Dr. Nikitin demonstrated that, in a distributed system where multiple computer nodes executed the same operations, it could be more efficient for a single node to execute an operation, while generating a proof of correct execution, and to convince the other nodes of this correctness by letting them verify the proof. To achieve the required efficiency, Dr. Nikitin co-developed multiple complex cryptographic techniques to reduce the cost of proof generation and verification. This was a groundbreaking result because the research community had previously considered outsourced verifiable computation to be a high-overhead tool that inevitably caused efficiency decline. The demonstration that this tool could, instead, improve efficiency was a landmark advancement in the field.

The result above also had a profound practical impact. The modern example of RSMs are blockchains systems, a recent technology that has applications in finance, governance, and regulation. Dr. Nikitin showed how his techniques could be applied to Ethereum, the second largest cryptocurrency and a platform with the market cap of $400 billion. Concretely, they could increase the throughput of the Ethereum network fivefold which would translate in millions of dollars on saved transaction fees. Several cryptocurrency solutions later adopted and deployed this approach. Retaining researchers, such as Dr. Nikitin, with a deep expertise in new developing technologies is critical for the United States to maintain its position as the world technological leader.

As further evidence of his international recognition in the field, Dr. Nikitin's work has been published in the most prestigious conferences and journals, including IEEE Symposium on Security and Privacy, USENIX Security Symposium, Privacy Enhancing Technologies Symposium, and ACM Transactions on Embedded Computing Systems. Due to the fast pace of the field, conferences are the primary publishing venues for computer security and privacy researchers. The conferences in which Dr. Nikitin has published are commonly regarded as the most selective and impactful in the field. Moreover, Dr. Nikitin is a highly cited researcher, meaning that others in his field have found his work to be novel and useful

for their own research. At this time, his original work has been cited 330 times by researchers from around the world. Considering that most scientific papers are scarcely cited, this is a clear indication of the significant and worldwide impact of Dr. Nikitin's research.

In sum, researchers of Dr. Nikitin's caliber are extremely rare. His superior expertise and success of his research endeavors make him an invaluable asset to any employer or any country that hosts him. For these reasons, I strongly encourage your approval of this petition.