Dear Faculty Selection Committee,

I am writing to enthusiastically recommend Dr. Jesse Sowell for the role of Lecturer in Security and Crime Science associated with the Dawes Centre for Future Crime. I have known Jesse for five years. When we initially met in person at a RISCs Workshop in 2018. I was immediately impressed by Jesse’s nuanced comments that integrated dynamics in Internet operations, governance, cybersecurity, and policy. Based on his comments on bridging the gaps between operations and policy, I made sure to continue the conversation with Jesse at the dinner after the workshop. Since then, Jesse and I have kept in touch on common research interests, and I have gotten to know his background and research. Jesse is fundamentally interdisciplinary, integrating a background in political economy, Internet operations, and management to analyze and evaluate “bottom-up” cybersecurity as a distinctly sociotechnical problem. Jesse not only understands the standard technical coordination and collective action problems endemic in cybersecurity, but his on-the-ground engagement with actors securing the Internet’s infrastructure and services we use on a day-to-day basis is both unconventional and refreshing. He brings a distinctly pragmatic and realistic approach to understanding the real-world incentives involved in improving Internet security, reducing cybercrime, and making these processes tractable and sustainable.

*Your brief bio and why you are qualified to evaluate my fit for Security and Crime Science; Shane certainly knows this, but the others on the committee might not know how awesome you are ☺*

Of particular interest is his research on reputation in the anti-abuse community, and how that work can be adapted to a system-of-systems approach to IoT reputation. Jesse has demonstrated a deep understanding of how cybersecurity operators use reputation indicators to minimize cybersecurity and cybercrime threats such as phishing campaigns and malware distribution. His work goes beyond the technical mechanics to explain precisely how the norms, best practices, and standards governing the use of these indicators are developed and maintained, and how these communities balance the incentives of the public and private actors involved to create security a collateral public good. In June of 2018 Jesse invited me to attend the Messaging, Malware, and Mobile Anti-Abuse Working Group’s (M3AAWG’s) annual European meeting in Munich. I had the opportunity to observe Jesse’s engagement with these communities firsthand, both in general sessions and a joint session that we ran to kick off M3AAWG’s IoT Special Interest Group. I was impressed with the depth and breadth of access Jesse has developed with this important community, as well as the level of rapport and respect Jesse has garnered for his work and contributions as both a researcher and the pragmatic application of his research to anti-abuse governance, the promotion of cybersecurity norms and best practices, and reducing cybercrime.

My recent engagement with Jesse has focused on his sociotechnical model of IoT security. Like his work on IP address reputation, this work integrates the technical requirements of such a system and the factors contributing to (and limiting) the institutional supply and demand for IoT security indicators, best practices, and standards. He tempers these models with a realistic analysis of the incentives of the actors in the IoT value network. In contrast to the abundance of mostly theoretical models of Internet security, the tractability and real-world incentives necessary for industry and governments to co-produce Internet security are primary drivers in Jesse’s work. Jesse demonstrates this approach in his article with Dr. Irina Brass from STEaPP on adaptive regulatory governance design for the IoT. He effectively integrates his work on planned adaptation and how cybersecurity knowledge is created and disseminated to make a valuable contribution to how IoT regulation and standards can keep pace with continuous innovation by cybercriminals. In particular, his arguments for sustainable commitments to operations-policy interfaces that facilitate incorporating on-the-ground cybersecurity expertise into the development of IoT security standards and regulation is an extremely important contribution that highlights both current gaps and represents an innovative approach to evidence-based policy making that can improve security and reduce the opportunities for cybercrime.

Of particular interest to me was the overlap between Jesse’s formulation of reputation indicators in the wild---essentially the track record of a device and brand’s security---with my own work on continuous testing of IoT device security and the role of home routers in IoT security (PITCHR). Both of our respective workstreams highlight the need to continuously re-evaluate the security of IoT devices after they have left the lab, i.e. in deployment. Jesse’s model also showcases his mixed methods approach to developing realistic, empirical models of IoT security. Jesse combines (1) his technical understanding of Internet and cybersecurity operations and (2) how technical indicators are created, interpreted, and what they can (and cannot) tell the analyst about malicious behaviors, with (3) his extensive knowledge of actor incentives to articulate the data collection trade-off space in terms of the costs and incentives of those directly involved and broader policy issues such as the tension between privacy and security. The mix of skills necessary for this deep, yet bottom-up, system-of-systems approach to IoT security is quite rare and valuable. To formalize this collaboration, I have invited Jesse for a paid summer research fellowship with my Sociotechnical Cybersecurity group to further develop this work, building on both his work, our work on optimization and simulation approaches to cybersecurity, and the PITCHR project. Jesse will be working with us to refine and integrate our respective models of IoT security as well as develop grants to continue this work, and, in particular, further develop relationships with ISPs in the US and the UK to identify a path to testing these models in the wild.

Although I cannot speak to Jesse’s teaching in his current posting, he has visited my research group when he has been in the UK for his own research and his honorary lectureship in STEaPP. On each occasion, Jesse’s presentations to my group were clear, compelling, and engaging. My students and postdocs enjoyed discussing his work and the overlaps of their work with Jesse. He is a genuinely intellectually generous scholar that is keen to collaborate with others.

I am enthusiastically looking forward to my collaboration with Jesse this summer and highly recommend Jesse for the role as Lecturer in in the Department of Security and Crime Science. I believe his interdisciplinary background, grounded in the principles of engineering systems and political economy, is an excellent fit for your department’s research and teaching, in particular the Dawe’s Centre’s work on cybercrime, IoT, and consumer safety. I believe Jesse’s intrinsically interdisciplinary background would make him an excellent advisor for your students, in particular PhD students in the Cybersecurity Doctoral Training Programme. Please do not hesitate to reach out to me if you have any questions regarding this recommendation.