EXECUTIVE SUMMARY

1GCYBER submits a proposal that will add value to Latin America and the Caribbean. Our influence for this proposal stems from Mr. Fraser's research on "Cybersecurity skills as a driver for economic growth in developing nations." This research explores the current issues prohibiting skills development, cybersecurity challenges, and the impact of cybercrime on national economic sectors. 1GCYBER specifically seeks to strategically deliver on key challenge areas: a) limited regional cybersecurity skills b) national and regional cybersecurity challenges, c) how cyber-crime impacts each regional state, and d) existing legal structures and gaps for operational management. These four themes will tactically serve as a light house towards which the training will be delivered to prepare highly trained practitioners.

The proposed courses will help to conjure critical thinking about the region's future cybersecurity needs as Latin America and the Caribbean advance economic and national security. As a known national imperative, the ability to combat cyber-crime and strengthen cyber resilience is essential to improving national economic and social development. The existing risk management frameworks echo economic security as a foundational pillar for domestic growth. Cybersecurity addresses the inherent risks to critical infrastructure and services resulting from the use of information and communication technology. The developed nations, specifically the United States, Britain, and Canada, recognize the importance of critical infrastructure systems. They continuously develop strategies that include cybersecurity education as a measure to protect cyber-physical systems.

The lack of a workforce with the requisite cybersecurity skills is a phenomenon that exist within the region and that which 1GCYBER commits to support through superior training. Latin America and the Caribbean's focus on cybersecurity skills forms the necessary foundation to correcting the current cybersecurity challenges and impact of cybercrime on the region. The issue varies from country to country. However, each presents a case that fosters critical thinking, influencing decision making and policy. This training proposal stems from a thorough understanding of the elements set forth in several national cybersecurity and cybercrime action plans. 1GCYBER will ensure that all participants understand cybersecurity through the doctrine of risk management. The proposed curriculum will adequately address the system dynamics of cybersecurity, cybercrime, education, and national security functions.

Professionals across Latin America and the Caribbean will leave with the requisite knowledge, skills, abilities, and core competencies to adopt and implement recommended best practices. 1GCYBER will ensure that training addresses these thematic elements from a global and Latin America and the Caribbean Community perspective. Apart from training and sharing of experiences, the proposed courses will draw attention to the need for knowledge about the instrumental value cybersecurity skills. Policymakers, stakeholders, educators, and citizens of the region, and other similar developing countries will benefit from this opportunity. 1GCYBER will

seek to influence a regional cybersecurity community, through services that encourage participating professionals to continuously collaborate, study, and work on their administrative and technical cyber capabilities. Apart from the proposed training, participants will be encouraged and given relevant resources to pursue certification, which serves as an attestation to their new abilities.

1GCYBER understands the regional skills and technical resource landscape. We anticipate there will be a mixture of skilled professionals and will make modifications to the proposed curriculum based on the average capability. This risk will be managed early by ensuring all participants across the two lots are given core knowledge, skills, and abilities (KSA). 1GCYBER's training is influenced by the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework and the Chartered Institute of Information Security's knowledge, skills, and roles frameworks.

1GCYBER will also encourage leadership and teamwork as a form of developing those non-technical skills that the literature critique as missing from current frameworks. Participants will be encouraged to complete free industry training from edX (Linux), Splunk (Reporting), and AWS (Cloud). These serve as essential knowledge and inputs to the Advanced Cybersecurity Skills Framework but are not a mandate. The proposed courses will implement these structures. Another vital risk to address is participant computing devices. Participants must have devices capable of installing virtualization technology, and Linux and windows virtual systems. 1GCYBER will address this risk by encouraging teamwork, in Zoom breakout rooms, where all participants collaborate on lab work.

Thank you,

Dr. Dustin Fraser, CASP, SSCP

Director, 1GCYBER