Distinguished guests, attendees, sponsors and partners - Good Morning, - Might I add to ensure that I cover all bases the all encompassing *All protocols observed.*

I would like to begin by commending the Mona ICT Policy Centre for conceptualising this two-day conference on a national problem and bringing together key stakeholders to discuss the issues arising around Cyber Security and Digital Forensics and formulate strategies towards a solution.

Henlin Gibson Henlin as a firm of attorneys with a keen interest in ICT is privileged to be associated with this effort.

This conference takes place in a national context about the nature of a global network, the internet that was gifted to the public, *the citizen*, in the mid-1990s when it was placed in the public domain. The conference also comes against the backdrop of its misuse which threatens the viability of critical infrastructure and the national image.

Cyber security is a subject matter of concern because the internet is inherently vulnerable and unsecured. This is because of its decentralised design in the sense that structurally it is neither owned nor controlled by anyone. This contrasts with private networks that are more proprietary and have more security built into them and are

operated on the assumption that there is likely to be some form of unauthorised access or intrusion.

Insecurity as a feature of the internet makes this conference on Cyber security an imperative. This is so because the private networks that run critical infrastructure such as banks, the electric grid and other utilities require access to the citizen and must be connected to it and by virtue of that fact are at risk.

The more information driven the society becomes, the more the risks increase so that as Richard Clarke, points out in his book *Cyber War: The Next Threat to National Security*:

> "The same way that a hand can reach out from Cyberspace and destroy an electric transmission line or generator... [it can], ... reach out from cyberspace causing things to shut down or blow up, things like the power grid, or a thousand other critical systems...

These critical systems can be financial systems, telecommunications networks and networks that run government business. We have recently had three highly publicized local examples one of which was a repeat incident. On other occasions incidents occur just to demonstrate that the hackers can do it, and then the attack suddenly stops. That is why the lessons from this

conference must be taken seriously, since a total shut down has not happened here yet or at least as far as I am aware.

This security problem makes this conference an important venue for raising awareness and creating a culture of responsibility in the use of the internet and protecting identity.

It would be remiss of me were I not to address the other aspect of the conference that speaks to Digital Forensics. Digital Forensics is basically the application of computer techniques to evidence so that it is acceptable in legal proceedings.

This is extremely important since computer science was once thought to be the domain of the IT security specialist. I recall being asked in about the year 2000 *what I was doing* in a course on computer security right here in Jamaica. Today collaboration between lawyers, computer and other IT experts is required to secure a conviction in relation to the commission of a cybercrime. You might have heard that since the passage of the Cybercrimes Act in 2010 there has been only one successful prosecution.

Digital Forensics is also useful in investigations to identify the perpetrators. A famous example of it being instrumental was its use by investigators to identify the Boston Bombers.

Currently, there is grave concern about the increase in cybercrimes and whether the penalties under the existing Cybercrimes Act are a sufficient deterrent.

I would like to suggest, that one of the greatest deterrents is effective enforcement mechanisms in terms of the capacity for successful prosecutions and therefore punishment. The focus on Digital Forensics at this conference is to train attention on the importance of capacity building of a cadre of expertise to handle digital evidence.

It is against this background that the conference ends on an important note – with the drafting of training and reform proposals for cyber security and digital forensics.

On behalf of the organisers, partners, stakeholders and the Mona ICT Policy Centre I cannot say enough how grateful I am that you are here and to echo the welcome and also to encourage your engagement and discussion.

I thank you.