Executive Summary
(State of Qatar)

The State of Qatar recognized some time ago that information, or cyber security is not just a technology issue, but also a matter of national policy. To this end, Qatar’s Computer Emergency Response Team (Q-CERT) formed in 2005 to catalyze change, and more specifically to accelerate the widespread adoption of effective cyber security practices and policies, and now has a National Mandate to safeguard State of Qatar digital assets.

In 2013, the Prime Minister of Qatar formed a national Cyber Security Committee. The committee has developed Qatar’s National Cyber Security Strategy in order to improve Qatar’s security posture and ensure the continued success and growth of the nation through five pillars that determine where action will be taken:

- Safeguard the national critical information infrastructure;
- Respond to, resolve and recover from cyber incidents and attacks through timely information sharing, collaboration and action;
- Establish a legal and regulatory framework to enable a safe and vibrant cyberspace;
- Foster a culture of cybersecurity that promotes safe and appropriate use of cyberspace;
- Develop and cultivate national cybersecurity capabilities.

Q-CERT has been successfully delivering different information security services to meet the needs of our constituents, businesses and organizations especially in the areas of incident response, intelligence, resiliency, training and awareness, crisis management, public key infrastructure licensing and identity, and the creation of the National Information Security Compliance Framework.

We believe there is currently a gap in the ability of states to gain and share sufficient cyber situational awareness at regional and international levels to enable effective decision-making. We need more work on collaborative prevention, to ensure stronger cyber security across cyber infrastructure and services to ensure resilience, especially in regards to the normal operation of daily life for governments, services, businesses, consumers and citizens.

Cyber Security has never been more efficient that when information exchange is taking place. Working on Information Sharing Agreements would be a great asset for states through collaboration frameworks that describe verification and compliance methodologies.

Attacks will happen and nations, governments, organizations and industry must be prepared, together.

For further information, please visit www.Qcert.org