

From: **Du Plooy, Emmerentia E**

Date: Thu, Apr 6, 2017 at 5:43 AM

Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Good day

My organisation is a Member of the Information Security Forum (ISF), which is an independent, not-for-profit organisation specialising in cyber security. Like many other ISF Members we make significant use of the ISF's Standard of Good Practice for Information Security (ISF Standard) to help manage information risk and meet the requirements of a range of standards, including the NIST Cybersecurity Framework (NIST CSF).

The ISF Standard provides complete coverage of the NIST CSF (as well as other standards, including ISO/IEC27002, COBIT 5 and PCI DSS) and is supported by comprehensive cross-references to the current Cybersecurity Framework. For this reason, we have reviewed the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity and wish to submit the following comments.

The Informative References column in the Framework Core needs to include references to the relevant topics as covered in the ISF Standard. This will help us to demonstrate how these two standards are aligned (e.g. to executive management, operations staff and suppliers). This alignment has become critical to our business partners especially during risk treatment discussions.

Reference material to support this request is available from the ISF. The ISF contact is Mark Chaplin, who can be reached by email at, by telephone or by post at Information Security Forum Limited, 10 Eastcheap, London EC3M 1DE United Kingdom.

We look forward to the inclusion of the references in the next release.

Kind regards

Emmerentia du Plooy

Group Information Risk Office / Head of Information Risk Governance

www.standardbank.com