

Ref. No. SGF/OP/II/S.3/T/8

10th July, 2012

The Head of the Civil Service of the Federation,
Office of the Head of the Civil Service of the Federation,
Federal Secretariat, Phase II,
Shehu Shagari Way,
Abuja.

**GUIDELINES ON THE RELATIONSHIP BETWEEN MINISTERS AND
PARASTATALS OR GOVERNMENT-OWNED COMPANIES**

I am directed to acknowledge the receipt of your letter Ref. No. HCSF/PS/CSO/556/II/107 of 27th June, 2012 on the above subject and to inform you that appropriate action is being taken thereon.

2. Please accept the warm regards of the Secretary to the Government of the Federation.

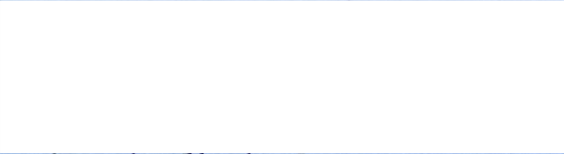
'Femi Olayisade, mni
Permanent Secretary (GSO)
for: Secretary to the Government of the Federation

SGF,

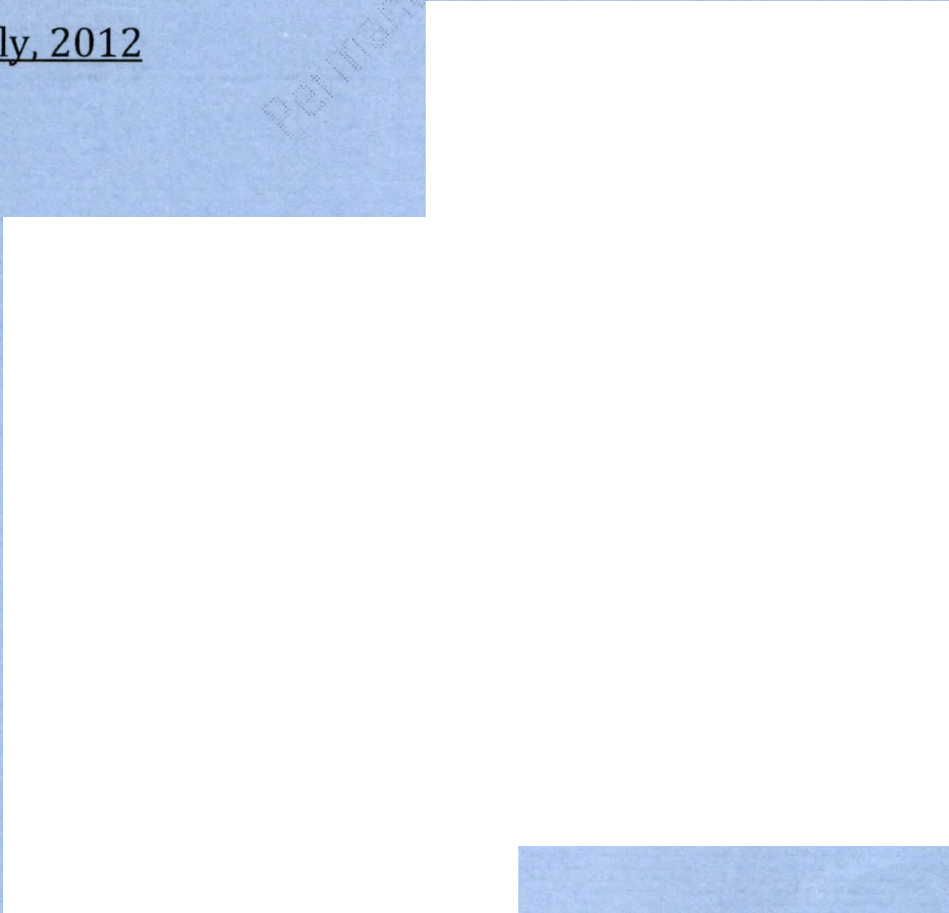
As directed at page '4', the letter from the Head of the Civil Service of the Federation has been acknowledged at page '8'.

2. In addition, please find *abc* a draft Circular for your consideration.

3. Submitted, please.


'Femi Olayisade, mni
Permanent Secretary (GSO)

10th July, 2012



SGF

**RE: NEED FOR USING THE ng. DOMAIN FOR
WEBSITES AND EMAIL ADDRESSES**

I respectfully, wish to refer you to the attached Report from the Department of State Services (DSS) and the Ministry of Communication Technology's response letter, on the above subject matter.

2. The DSS reported that the Jam'atul Ansarul Muslimina Fil-Biladis Sudan (JAMBS), a splinter group of Jama'atul Ahlis Sunnah Li-da'awati Wal-Jihad, led by Anas Ibn Umar directed its Information and Communication Technology (ICT) Unit, to hack the computer network of expatriates and important personalities in the country in order to monitor their itineraries in order to facilitate their kidnap for ransom. The Sect also planned to use insiders within the telecommunication sector to obtain information for the operation.
3. This development could challenge Federal Government's resolve to guarantee the safety of its personnel and public installations. Hacking of networks by the terrorist group could avail them the opportunity to access sensitive information of expatriates, and highly confidential information of Government which their unauthorized disclosure could cause harm to the interest of the country.
4. Consequently, the Ministries of Communication Technology, Science and Technology and the Inspector General of Police were appropriately intimated of the DSS's report on the subject matter, and were advised on the need to emplace appropriate security measures to safeguard Government personnel and confidential information as well as expatriates in the country. In response, the Ministry of Communication Technology advised that the important personalities/expatriates should be persuaded

to take advantage of the very secured Service-wide shared services platform for their On-line presence and activities as a first measure in beating the potential hackers i.e. the .ng. domain should be used for their websites and emails addresses. Furthermore, it recommended that the potential victims to constantly change their passwords as additional measure to frustrate the hackers from achieving their objective. In conclusion, the Ministry called on the SGF to issue a Service-Wide circular to enlighten public servants on the threat.

5. In view of the foregoing, this Office endorses the need for the SGF to issue a circular letter for MDAs to take advantage of the security provided by .ng domain as recommended by the Ministry of Communication Technology. The SGF is therefore, invited to note the foregoing for consideration and approval to enable compliance. Subject to your approval, you may please wish to consider the attached draft circular letter on the subject.

6. Please accept as always, the assurances of my highest esteem and loyalty.

Esther G. Gonda
PS SSO

19th July, 2013