Communiqué from the
'Strengthening the cyber security of our essential services' event

Ministers, senior representatives from lead Government Departments and regulators came together today to address the challenges posed by cyber security to the essential services on which we all rely.

Cyber security is a top tier national security priority for the UK Government.

In line with the 2011 UK Cyber Security Strategy, work is underway across Whitehall and industry to ensure key data and systems continue to be safe and resilient in our critical national infrastructure.

Our essential services are increasingly reliant on cyber systems and networks. Whilst this brings great opportunities it also brings challenges for their security and resilience. Government and regulators alike have a responsibility to help the companies which own and operate our essential services address these challenges.

Together we recognise that:

- Cyber systems and networks form a substantial part of UK infrastructure, underpinning many of the services used in UK daily life, from functions as diverse as financial payments to rail signalling. The use of such systems brings benefits to the consumer and the companies which deliver these services alike: driving greater efficiencies and enabling access 'on demand.' However, disruption to these cyber systems and networks can quickly lead to disruption in the real world: power failures, travel delays, late payments.

- To reduce the potential for disruption to these services, we all need to ensure the firms and markets that own and operate this cyber infrastructure have strengthened cyber security in place. Strong cyber security in the firms and markets we oversee is fundamental to meeting regulatory objectives, for instance helping to protect consumers (by helping to protect their data), helping the orderly running of markets (by increasing operational resilience of firms) and helping with the security of supply (by increasing the resilience of markets).

- Given the inherently international nature of the cyber systems and networks which support these essential services, there is a need to work with international partners to understand our risk and increase the level of network and information security, including at the EU level.

To take forward this agenda, Government and regulators will:

- Work to **embed cyber security in the firms and markets that they oversee** (including encouraging firms to: undertake a self-assessment against the '10 steps'; take up membership of the Cyber Security Information Security

Partnership, or CISP; manage cyber risk in their supply chains by driving adoption of the HMG Preferred Organisational Standard for Cyber Security);

- **Assess the state of cyber security across each sector**, on an ongoing basis, and work with industry to address vulnerabilities where appropriate;
- **Identify aggregated cyber security risks** within and across sectors, enabling the management of cyber risks affecting a number of entities;
- Working with industry, **increase information flows** on threat, vulnerabilities and mitigation strategies across each sector;
- Support sectors to develop effective **incident detection and management capabilities**, including working with partners (including CERT-UK) to develop, deliver and participate in appropriate **exercise programmes** for each sector.

These steps represent a common set of activities that will be taken forward between Government and relevant regulators in each area of essential services subject to the regulators' statutory duties. Reflecting the different nature of each sector, additional activities may be necessary to provide appropriate cyber security.

HM Government

Department for Transport

Office for Nuclear Regulation
An agency of HSE

BANK OF ENGLAND

FCA
FINANCIAL CONDUCT AUTHORITY

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Ofcom

ofgem
Making a positive difference
for energy consumers

OFWAT