Home Office

Critical Information Infrastructure Protection, identifying and sharing best practices

16 September 2021

Jerry Ketteringham

⁺Security through Partnership

Background to the work of our team

A small cyber security team within the Home Office specialising in Government-to- Government partnership projects focusing on the transfer of best practice, skills, tools and methods.

Since 2017 our focus has been on helping countries conduct National Cyber Risk Assessments (NCRA) for CNI to help inform Critical Information Infrastructure Protection at the national level.

Our recent focus has been to develop an integrated package of support to help countries generate more effective National Cybersecurity Strategy by bringing together the insights from the NCRA, Oxford University Capacity Maturity Model assessments and the GCI.

Home Office

Helping countries take a strategic cyber capacity building journey

National Risk Assessment and CNI/CII dependencies

Help countries to conduct an 'all threats & hazards' risk assessment

Cyber assessments and strategy development

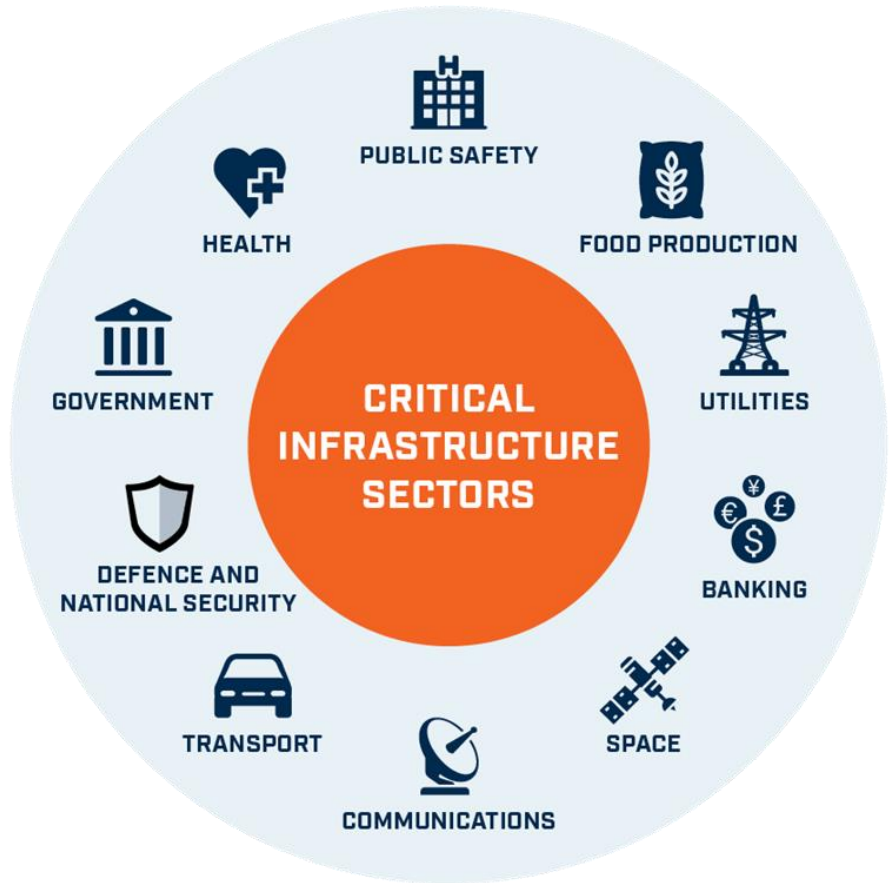Help countries to conduct NCRA and CMM assessments. And shaping an effective NCSS

Cyber capacity building

Priorities and recommendations for cyber capacity building initiatives

Capacity building training

Skills, CNI/CII protection, exercising and testing, incident management and countering cybercrime
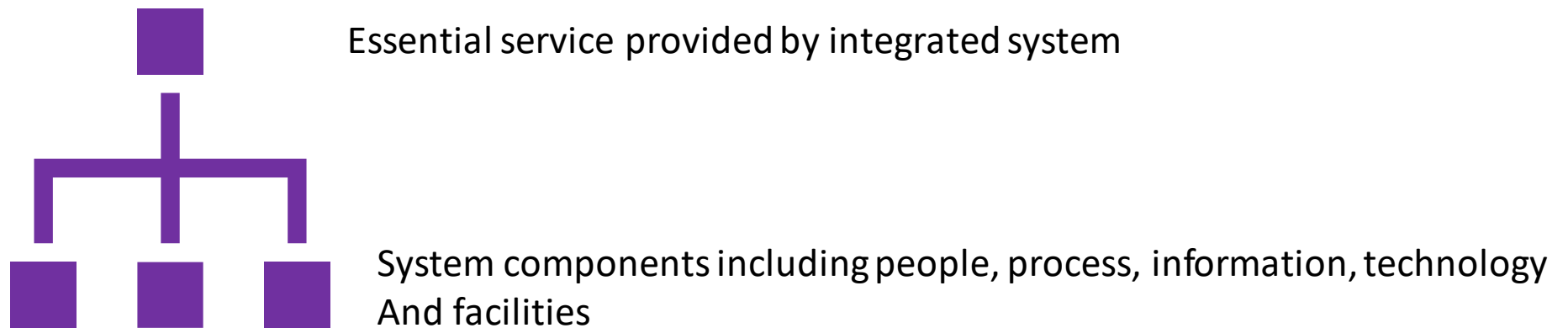
Home Office

Understanding CII risk

Overall impact					
5	0	3	3	5	4
4	1	4	13	11	7
3	3	12	18	23	8
2	3	5	11	16	5
1	18	9	6	4	7
	1	2	3	4	5

Overall likelihood

Taking a broad view of impact

Economy

Citizen

Health

National icons

Essential services

Reputation

Public trust & confidence

Working at the service/integrated system level

Essential service provided by integrated system

System components including people, process, information, technology And facilities

Home Office

Understanding CNI dependencies
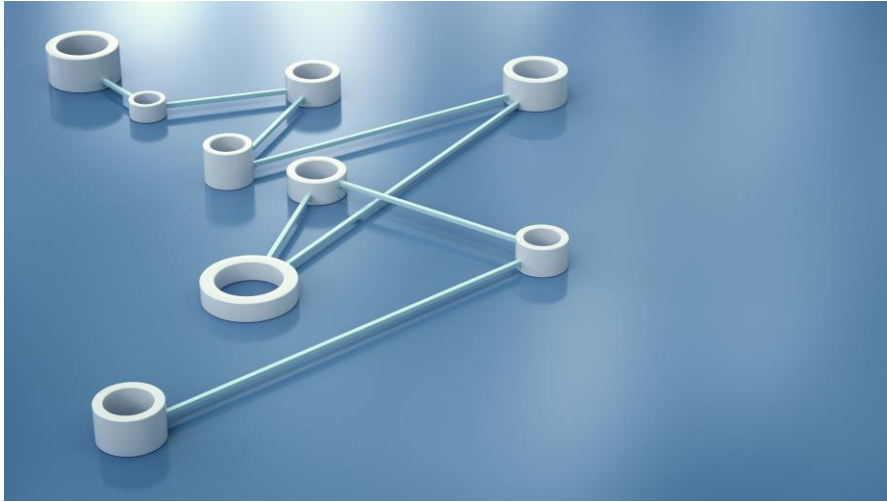
Intra and inter-sector dependencies can be difficult to capture. But it is essential to gain an understanding of these
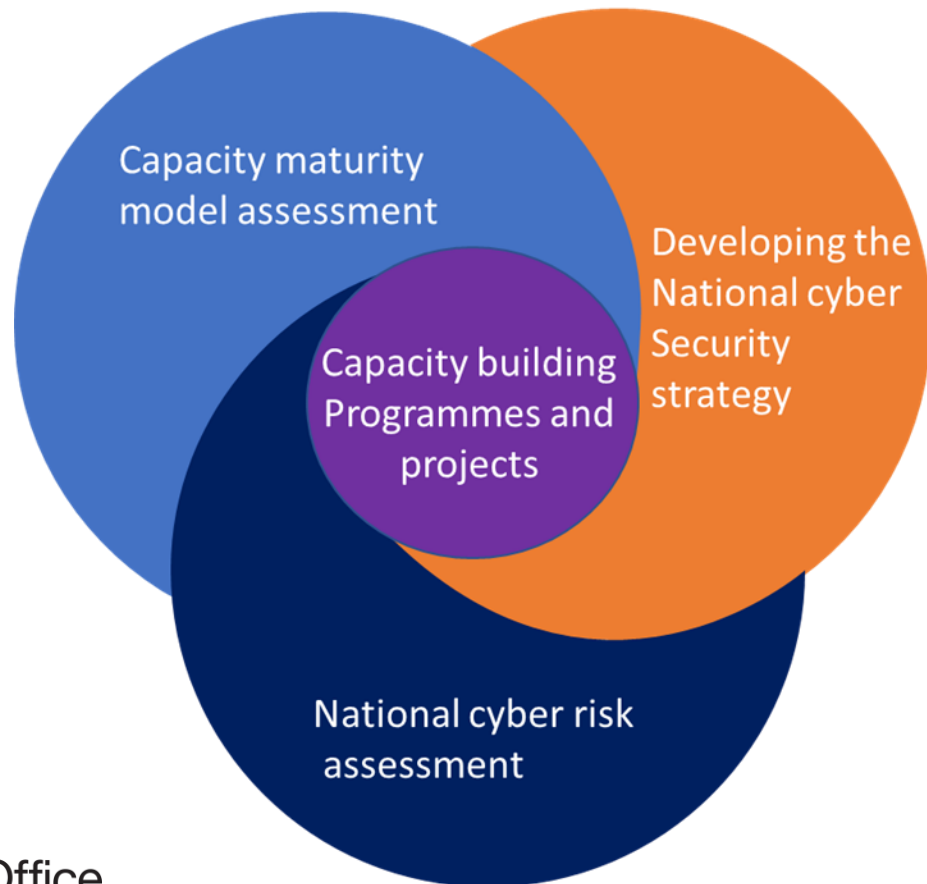
CNI dependencies are increasingly international and it is important to understand the cybersecurity risks from international supply chains

In 2020 the UK team developed and tested a methodology for capturing and assessing international CNI dependencies

Home Office

The national CII risk assessment can be integrated with other assessments to help shape National Cybersecurity Strategy

CMM, NCRA, NCSS and NCSP

Capacity maturity model assessment

Developing the National cyber Security strategy

Capacity building Programmes and projects

National cyber risk assessment

Managing CNI/CII risk is a core element of a National Cybersecurity Strategy.

The Joint Integrated Cyber Analysis Project (JICAP) in partnership with the ITU and Oxford University has developed a methodology for bringing these initiatives together.

Home Office

Summary of good practice

Make cyber risk to the CNI part of the top tier national risk register

Use a National Risk Assessment process to help identify and characterise CII and Essential Digital Services

Use a national definition of impact levels to determine what is CII

Take a broad view of what constitutes a national impact

Gather risk information at the service and integrated system level

Consider CII dependencies and supply chains at the national and international level

National CII risk assessments and cybersecurity maturity assessments can be integrated to help shape and inform National Cybersecurity Strategy

Home Office