CPNI
Centre for the Protection of National Infrastructure

Asset Identification Guide

PUBLISH DATE: July 2020

CLASSIFICATION: Official

In addition to ensuring appropriate leadership and governance structures are in place to assess and manage protective security risks; organisations must seek to understand what assets of value they hold in order to design and implement proportionate and effective security measures for their protection.

This Asset Identification Guide has been developed to assist anyone responsible for identifying an organisation's critical assets as part of the Protective Security Risk Assessment process.

Differing operational focus, operating environments and asset types of value will be indicative of the range of threats (the intent to inflict harm), threat actors (the hostile with mal intent) and threat vectors (the means of realising the threat) arrayed against organisations.

All organisational assets and systems that are necessary for the delivery of effective operations or are of specific organisational value (e.g. commercially sensitive information), should be identified. These may be: physical items, data stored or transmitted in any format (e.g. hard or electronic copy), personnel with specific knowledge/skills, or crowded places requiring protection. Engaging a suitable organisation-wide stakeholder group to conduct this exercise and provide ongoing support to the risk assessment/management process, will provide the greatest benefits.

It is not possible to provide a comprehensive list as different organisations and their operations may be dependent upon a range of unique and bespoke assets that require protection. It is also the case that different organisations may place different values on similar assets, dependent upon what they need to protect and why.

However, to assist in considering what might constitute an asset of value, organisations may wish to review the table provided at Annex A as a prompt for the generation of broad thinking and discussion.

To support effective risk assessments, and risk management decision making, it should be noted that assets may vary in value, indeed the value of some assets may change over time and should therefore be subject to review as dictated by circumstances, such as operational, environmental or threat changes

Annex A

Potential Organisational Assets of Value

Organisations should consider what, if stolen, damaged, divulged or has it's confidentiality, integrity and/or availability compromised in any other way, may cause:

- **Reputational damage**
- **Financial damage**
- **Injury or loss of life to you, a stakeholder or partner, or the wider public**
- **Assist in furthering the aims of a malicious / hostile entity.**

Asset Type	Types of Information	Medium	Possible Examples
Information	• **Personal Info identifying individuals.** • **Sensitive info identifying specifics on individuals; medical, religion, financial details etc.** • **Commercial information strategic planning, 'trade secrets'.** • **Research Information may include any of the above plus intellectual property.**	• **Spoken word** • **Paper / Hard Copy** • **Electronic data** • **Storage & media** ○ **Servers** ○ **Hard drives** ○ **USB drives** ○ **Memory cards** ○ **Programmable memory chips** ○ **Phones** ○ **Watches** ○ **Multi-Function Devices (Photocopier/Fax/Scanner)** ○ **CD's** ○ **DVD's** ○ **Magnetic tape** ○ **Microfiche** ○ **Carbon/printer ribbons**	Maps Charts Plans Surveys Recipes Vetting information Biometrics

	• **Corporate information and partner information entrusted for a specific purpose.**	○ **Filing cabinets** ○ **Desktops & desk drawers** • **All medium in transit or awaiting destruction**	Photography (digital and wet film) Video (digital and wet film) Audio recordings (analogue and digital) Logs (incl of sensitive measurements) Carbon papers Historical examples of the above Copies, duplicates and back-up
Physical	• **Rooms** • **Buildings** • **Sites**		Secure storage facilities Server rooms Guard rooms

	• **Key process infrastructure (e.g. valves, pipes, storage)** • **Physical items of value**		Control rooms Reception areas Sensitive meeting areas Research facilities Restricted sites Areas adjoining the above with ability to provide access Physical products specific to organisation (e.g. 'widget') Restricted and/or controlled items including, but not limited to, arms, ammunition and/or explosives
Personnel	• **Key skilled / knowledgeable workers**		Individuals with unique knowledge and/or skills for which there is limited supply and

			organisational reliance
Other	• **Flora and Fauna** • **Assets of potentially limited financial value whose compromise may directly result in regulatory or reputational damage through use in criminal enterprise** • **Assets identified anywhere above controlled on behalf of a third party for which the organisation has a duty of care** • **Assets maintained or operated by third parties that may as a consequence result in them holding information or assets as highlighted through the above process (e.g. Organisational data with MSPs)**		Animals of value to continued operational capability (e.g. guard dogs, research assets) Unique plants Cutting equipment Liveried vehicles Uniforms Identity documents Organisational assets managed by others to fulfil contracts, manage services, or provide storage (physical or digital)