CPNI
Centre for the Protection of National Infrastructure

OPEN DATA: THE NEED FOR A SECURITY-MINDED APPROACH

SUMMARY

November 2015

The UK Government Open Data White Paper: Unleashing the Potential, published in June 2012, encourages public sector organisations to make it easier to access public data. There is a 'presumption to publish' unless there are clear, specific reasons (such as privacy, confidentiality or national security) not to do so.

However, in publishing open data, particular care should be taken to identify and protect information that could impact on the safety and security of:

- individuals;
- sensitive assets and systems; and
- the benefits which the sensitive asset or system exists to deliver.

In some cases the data may be geographically tagged, enabling its geospatial visualisation (e.g. open mapping), and thereby allowing relationships, patterns and trends to be more easily analysed.

In order to deliver this open data and to realise its intended aims, including the need to protect certain information, a security-minded approach is required which delivers:

- **safety** - preventing the creation, by the use of open data, of harmful states which may lead to injury or loss of life or unintentional environmental damage;
- **authenticity** - ensuring that the open data is genuine;
- **availability** (including reliability) - ensuring accessibility and usability of the data in an appropriate and timely fashion;
- **confidentiality** - ensuring control of access and prevention of unauthorised access to sensitive information;
- **integrity** - maintaining consistency, coherence and configuration of data sets;
- **possession** - preventing unauthorised control, manipulation or interference with systems disseminating open data;
- **resilience** - ensuring the ability of systems disseminating open data to transform, renew and recover in a timely fashion in response to adverse events; and
- **utility** - ensuring usability and usefulness of the data sets over time.

The security-minded approach

A security-minded approach should be adopted where a clear and specific reason for not publishing data exists, namely:

- to prevent an individual, or group of individuals, being identified or identifiable in the hands of a recipient of the data;
- to protect information about the location of sensitive assets or systems not otherwise generally visible directly or through other sources;
- to protect certain information pertaining to sensitive assets or systems, the location of which can be readily identified; and
- when the aggregation (through accumulation or association) of data, or an increase in the accuracy of the location of assets or systems, could compromise safety and security of an individual, an asset, a system or a related service.

Even where a data set has been anonymised or pseudonymised, care must be exercised to ensure that de-anonymisation is not possible, for example, where data aggregation allows restoration of identifiers or characteristics of a data set, leading to identification of an asset or individuals. There will be an additional security risk when this process would allow pattern of life analysis of certain

individuals to be undertaken using data collected over an extended period of time, thereby understanding that particular individual's habits and potentially predicting future behaviours.

The need for such an approach should therefore be assessed by the data owner, using an appropriate and proportionate risk management approach, prior to the release of a data set to a third party, and by the data publisher prior to:

- the publication of a new open data set;
- the update of an existing published data set;
- undertaking a review of an existing data set; or
- augmenting or linking a new or existing open data set with another data set.

Where there is any uncertainly as to the sensitivity of data, appropriate advice should be sought.

Open data - managing risk

Where the need for a security-minded approach has been identified, it will be necessary to develop a risk management strategy comprising a risk assessment, risk mitigation, and a process of review.

Risk mitigation measures that it may be appropriate to adopt include:

- removing a sub-set of the data from the published data set where only that sub-set creates a risk;
- reducing the precision of the information where the precision of location or timing data increases the risk;
- providing the data in summary form to reduce the level of detail available where the granularity of the data increases the risk;
- publish the data set without the metadata, or remove the sensitive fields, where the metadata creates a risk;
- monitoring access by requiring user registration/login to access specific data sets.

Where the data is used as part of an open mapping project, in addition to the measures above it would be appropriate to reduce the level of detail and/or remove some layers of mapped data as a user zooms in to view a locality where the granularity of the data increases the risk.

Further guidance

Further guidance on applying and implementing a security minded approach can be found on the website of the Centre for the Protection of National Infrastructure (CPNI) (www.cpni.gov.uk) or from your Departmental Security Officer.