british security industry association

Information Destruction in the Public Sector

Author: BSIA Information Destruction Section

Form 257
Issue 1
July 2015

Contents

Executive Summary

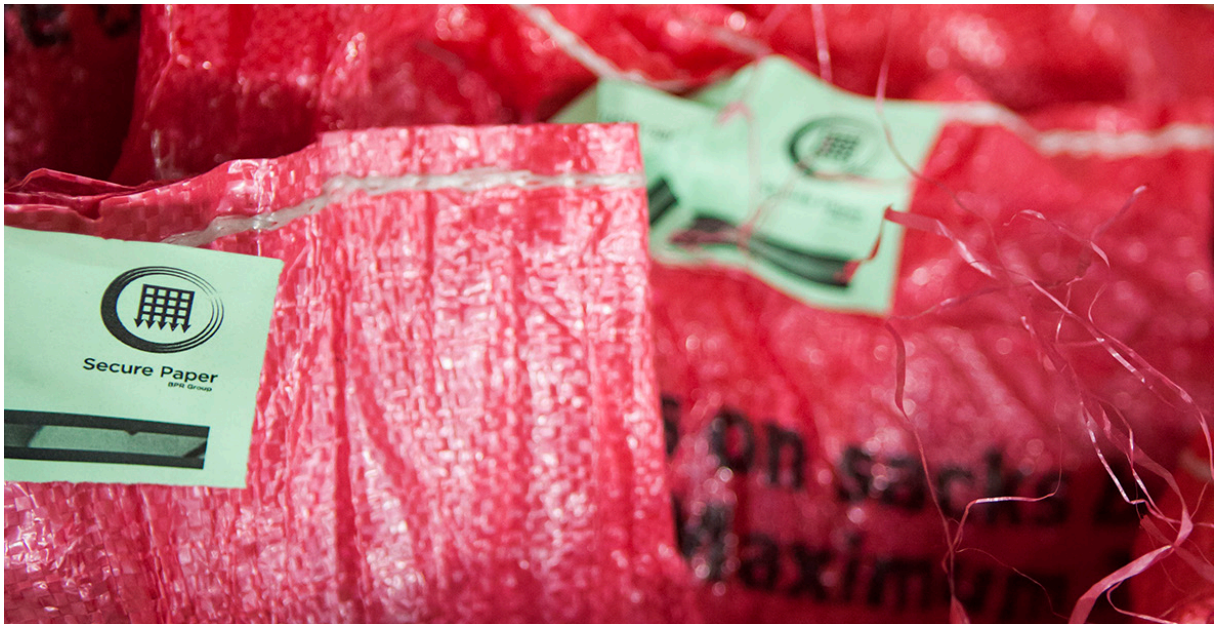
This paper is designed to provide guidance for public sector organisations specifying Information Destruction (ID) services. It references previously published guidance documents from the Cabinet Office, the Centre for the Protection of National Infrastructure (CPNI) and the BSIA Information Destruction (ID) Sector.

In August 2013 the CPNI published a new standard entitled *'Secure Destruction of Sensitive Items'*, which was prepared to provide procedures, processes and performance monitoring surrounding ID services that should be implemented by organisations belonging to the UK national infrastructure. At the time of publication the standard was intended to be applied to sensitive items assigned a protective marking (defined by the UK Cabinet Office) of CONFIDENTIAL, SECRET & TOP SECRET or an equivalent classification as determined by the item owner.

At that point in time, there were five levels of protective marking ranging from the lowest (PROTECT) to the highest (TOP SECRET) and the onus to classify the level of sensitivity lay with the item owner. In the absence of any other readily available guidance, some public sector organisations were liable to 'over specifying' ID standards within tenders. In particular, the classification of CONFIDENTIAL within this protective marking scheme was intended for information that was more sensitive than the day-to-day business of government, service delivery & public finances.

In April 2014, the Cabinet Office published new Government Security Classifications consolidating the five previous levels of protective marking into just three; OFFICIAL, SECRET & TOP SECRET. This led to a reclassification of existing marking levels across the public sector, a relatively simple task for those operating at the very highest and lowest classifications but more difficult for those operating in between.

These are significant events within the ID sector. In its capacity as a leading authority within the sector, the BSIA ID Section is consolidating these headline developments within this paper and – by engaging with CPNI – intends to deliver consistent guidance for all organisations when procuring ID services.



Scope

This paper is designed to enable organisations within or working with the public sector, and any organisation wishing to benchmark against that sector, to clearly determine the classification of data it is creating and therefore adequately specify the correct levels of secure destruction required.

Classifying Sensitive Materials

Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad range of threats. There are three levels within the latest UK Government Security Classification (GCS) system:

TOP SECRET

The Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations. Example - Iraq Weapons of Mass Destruction: Senate Report 109-331.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime. Example – Pending state visit agenda, certain foreign embassy records.

OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. 95% of all sensitive material created within the public sector is estimated to fall within this category. Examples – medical records, HR records, electoral registers, X-rays, invoices, payroll documents.

OFFICIAL Definition:

ALL routine public sector business, operations and services should be treated as OFFICIAL; many departments and agencies will operate exclusively at this level.

This includes a wide range of information, of differing value and sensitivity, which needs to be defended against the threat profile as described below, and to comply with legal, regulatory and international obligations. This includes:

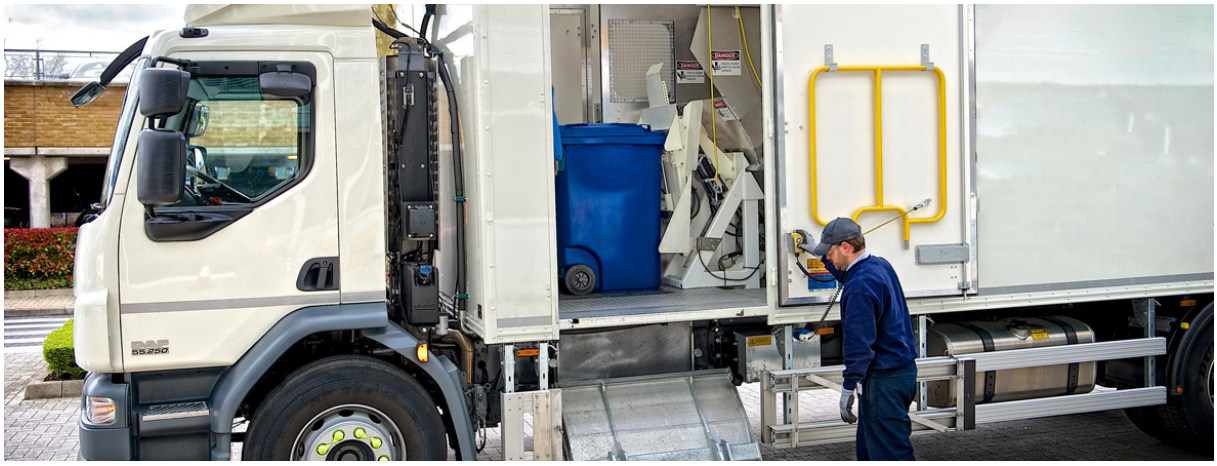
- The day-to-day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

NB. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may need additional security measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE'.

The three security classifications (OFFICIAL, SECRET and TOP SECRET) indicate the increasing sensitivity of information AND the baseline personnel, physical and information security controls necessary to defend against a broad profile of applicable threat:

The typical **threat profile** for the OFFICIAL classification is broadly similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend UK Government data or services against compromise by attackers with bounded capabilities and resources. There is no requirement to explicitly mark routine OFFICIAL information.

Data Owners are responsible for identifying any sensitive information within the OFFICIAL category and for putting in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements. Individuals should be encouraged to exercise good judgement and provide meaningful guidance on how to handle and destroy any sensitive information that they produce.



Specifying Information Destruction Services

Any organisation creating or working with information classified as SECRET or TOP SECRET should refer to the CPNI Standard 'Secure Destruction of Sensitive Items' when specifying ID services for these classifications.

The scope of CPNI's standard covers the following scenarios of destruction of sensitive items:

- Using static equipment at the location of use (item and destruction equipment co-located, such as a shredder in an office).
- Using mobile equipment at the location of use (destruction equipment is brought to the item).
- Transport followed by destruction using static equipment at an external destruction facility (the item is brought to the destruction equipment, such as use of a dedicated facility).

Whilst many departments and agencies will be operating exclusively at OFFICIAL level, there are likely to be examples where a single entity is creating two or even ALL levels of protective marking, often at the same site. The baseline set of security controls providing appropriate protection against typical threats for each classification must be adhered to and this will need to be taken into consideration when drawing up the specification for ID services.

The CPNI standard is prescriptive and sets out very clearly the baseline set of security controls that must be followed for classifications TOP SECRET and SECRET, from point of collection through to destruction outcomes.

The BSIA recommends that, for OFFICIAL (and OFFICIAL-SENSITIVE) classification, refer to the European Code of Practice for the Secure Destruction of Confidential Material, BS EN 15713:2009 to establish your baseline set of security controls.

Organisations may need to apply controls above (or below) this baseline on a risk managed basis appropriate to local circumstances and in line with the Government's risk tolerances. This is likely to be the case when considering the resulting destruction outcomes (shred size) for the materials being destroyed; and paper in particular, which is estimated to form the majority of OFFICIAL material created.

BS EN 15713:2009 is the European Code of Practice used to inform customers / end users as well as regulate the Information Destruction industry and includes a broad scope of destruction outcomes. As such it sets the baseline for Europe but in the UK the ID sector as a whole (shredding equipment manufacturers, outsourcing service providers & end users) are aligned behind a maximum 16mm cross cut shred size as being appropriate for 'commercial confidential shredding' including the new OFFICIAL classification.

When specifying desired destruction outcomes, factors for consideration may include but are not limited to:

- As a general rule, smaller shred sizes take longer to achieve due to slower shredding throughputs and require more advanced technology, both of which can drive up costs. The smaller the output required, the greater the cost to achieve it.

- Cabinet Office advice for OFFICIAL destruction states 'dispose of with care using approved commercial disposal products / services to make reconstitution unlikely by attackers with bounded capabilities and resources'.

- Where there is more than one paper waste stream, 'cross stream' contamination is a significant risk, e.g. in offices where there are general recycling receptacles, general waste receptacles and confidential waste receptacles, it is common to find every category of paper waste in every receptacle. Controls should be put in place to ensure sensitive waste is kept separate from general waste. In certain circumstances a total destruction policy may be more appropriate in order to 'manage out' this risk.

- Post-destruction conditions may be taken into consideration. Co-mingling shredded materials (whether done on or off site) from multiple sources makes reconstitution far less likely. It would be environmentally desirable to ensure that, following destruction, the destroyed material is recycled where possible.

- Holistic security and not over-reliance on the waste outcome (i.e. shred size). Procedural, personnel and physical security measures must work in together, especially in order to protect sensitive material when in storage or transit.

Further reading

Cabinet Office Government Security Classifications April 2014
Secure Destruction of Sensitive Items CPNI Standard April 2014
EN15713:2009 Information Destruction Complete Guide BSIA September 2014

For further information you can contact the BSIA at **www.bsia.co.uk** and visit the CPNI advice page here:
www.cpni.gov.uk/advice/physical-security/secure-destruction-of-sensitive-items

BSIA
Kirkham House
John Comyn Drive
Worcester
WR3 7NS

www.bsia.co.uk
email: info@bsia.co.uk
tel: 0845 389 3889
fax: 0845 389 0758