



Royal Canadian  
Mounted Police

Gendarmerie royale  
du Canada



## Presentation to NAID 2008

# Government of Canada Requirements for the Destruction of Classified and Designated Information

**Ken Clupp, CD, PEng, CTech, PSP**  
Senior Technical Security Consultant  
RCMP Technical Security Branch (TSB)  
Coordinator: Security Equipment Guide and Destruction Equipment Testing

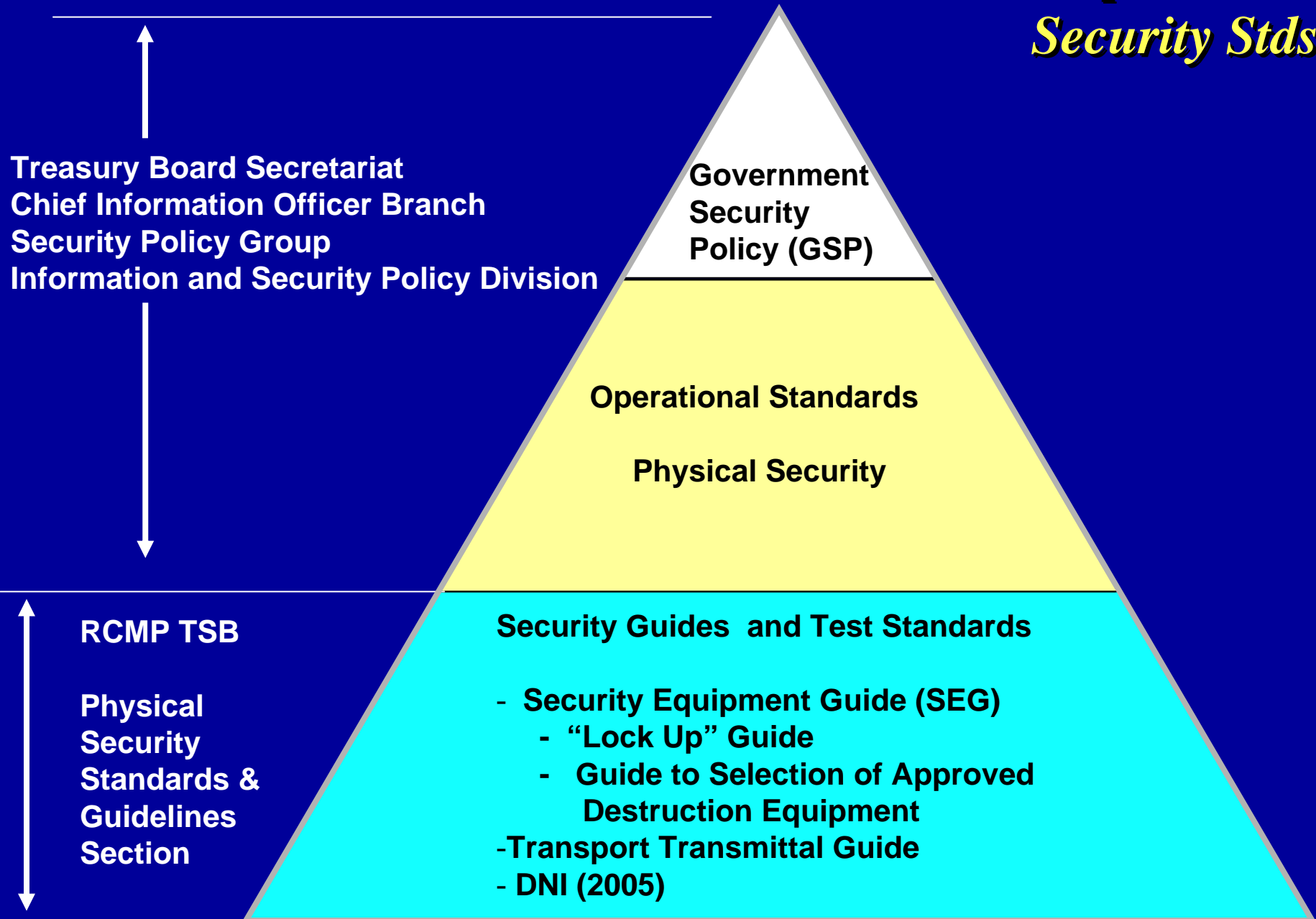
Co-presented by:

**Daryl Leach**  
PWGSC Canadian Industrial Security Directorate (CISD)

# Lead Agencies

- Government Security Policy (GSP)
  - lists 10 lead security departments and their responsibilities.
- RCMP TSB Responsibilities:
  - Provide advice and guidance on physical security
  - Conduct research and development
  - Develop policy and guidelines on physical security
  - Provide security training

# *TB Policies and Operational Security Stds.*



# Policy Hierarchy

- **Government Security Policy (GSP).**
- Requirements of Annex B to the **Operational Security Standard on Physical Security (2004)**
- **Destruction, National Interest - DNI (1985)**
  - Standard for Destruction Equipment Testing
  - Includes requirements for **Protected Info**
  - Applies to IT media (by ref to ITSG-06)

# Classified or Protected ?

- **Classified** information is that which concerns the National Interest.
- **Protected** Information (formerly Designated) concerns the individual person or corporate entity.
- Both are subject to exclusions under Access to Information and Protection of Personal Information provisions.

TOP SECRET  
TRÈS SECRET

SECRET  
SECRET

CONFIDENTIAL  
CONFIDENTIEL

PROTECTED C  
PROTÉGÉ C

PROTECTED B  
PROTÉGÉ B

PROTECTED A  
PROTÉGÉ A

Threats: unauthorized disclosure, destruction,  
removal, modification or interruption

# Confidential ≠ Confidential

- As used by private sector and non-federal governments relates to sensitive personal information
- As used by the Government of Canada (GoC) relates to information which – if compromised – would cause injury to the National Interest.
  - This is generally never private information relating to individuals or corporations
- GoC term for private and other non-national interest information is Protected
  - i.e.: Protected A, Protected B or Protected C

# Threat

- Unauthorized disclosure is the perceived threat for information and is the main focus of destruction equipment evaluation and approvals. Other risks may also apply to information on IT media. The adversary's anticipated method of attack is the restoration or analysis of the residue produced during the destruction process for paper and other text based media (such as microfilm), or by reconstruction or other restoration of data from components, parts or fragments of IT media such as hard disks and memory devices.
- Approved destruction equipment and processes make reclamation of protected or classified information impracticable (though not impossible).

# Limitations

- Approved destruction equipment for text-based media except micrographic is limited to:
  - **within Canada under normal threat conditions**
    - Destruction of information outside Canada or under heightened threat conditions may require additional measures as recommended by a **TRA**.
  - **font size is 12 point or larger.**
    - Destruction of text smaller than 12 point will normally require additional measures such as the use of a Type II (level 6) machine.
- Destruction of micrographic media must be by equipment specifically approved for that use.

# Types

- Approved destruction equipment and processes are limited to specified media and security classifications. The term “Type” is used to describe in a single term the security ratings by class of equipment for shredders and disintegrators for **paper**.
- Intent of varying Types is to set acceptable sizes (while maximizing throughput) so the chaff (particles) can be disposed of as unclassified waste. That is, **the adversary does not have time, technology or motivation to do what is necessary to put it back together again.**

# Paper Shredder and Disintegrator “Types” (GoC terminology only)

---

TOP SECRET

PROTECTED C

Type II

SECRET

PROTECTED B

Type III

CONFIDENTIAL

PROTECTED A

COTS

- **Type II:** a shredder or disintegrator approved for Secret, Top Secret and Protected C information
- **Type II (Level 6):** sub-category – designed to cover high security paper shredders and disintegrators meeting new NSA size standard. Recommended in our system for cases where a TRA recommends a higher degree of security (e.g.: embassies, overseas deployments, smaller than 12 point font text size or specifically targeted material).

**Note: although many high security shredders are NSA approved, only those listed in the RCMP SEG have been approved as meeting all RCMP Destruction Standard criteria. Only SEG-listed machines are assigned the Type II (level 6) designation.**

Type II (level 6) is a GoC term and only we can assign it or use it.

- **Type III:** a shredder or disintegrator approved for the secure destruction of Confidential and Protected B on paper (subject to a TRA).
- **Type IIIA and Type IIIB:** sub-categories of Type III. Type IIIA is for regular use and Type IIIB is for the destruction of information in bulk (only). Bulk Destruction (for Type IIIB) means the destruction of at least one ream (500 sheets) or approximate equivalent (such as a full refuse bag) in a single session.
- **Micrographic Media:** Destruction equipment must be specifically approved for micrographic media.

# Type II

Shredders: 1 mm x 14.3 mm

Disintegrators:

Approved on the basis of screen size.

Not greater than 6 mm (1/4") dia

# Type II (level 6)

- The National Security Agency (NSA) conducts its own program of shredder and disintegrator testing for the US government.
- The NSA size for all levels and conditions is 5 mm<sup>2</sup>
  - Our Type II size: 1mm x 14.3mm = 14.3mm<sup>2</sup>
- The size requirements of the NSA exceed our Type II requirements, but apply in ALL situations. They do not permit larger sizes for any classified material and do not have a formal equivalent to our Protected category.
- Our Type II size is approved to TS for 12 point font, in Canada under normal security conditions.

# Type III

Two sub-categories: Type IIIA and Type IIIB

- Approved (and this standard established) for the destruction of **Confidential** information on paper
  - max 12 point, in Canada, normal security conditions
- Approved for the destruction of Protected B, where a TRA has recommended the use of RCMP approved destruction equipment
- Also suitable (but not required) for Protected A

- Type III A – General office use
- Type III B – Bulk (high volume)
  - The size requirements take into consideration the effort required and motivation of the adversary. Given this, the risk to the information at a given size is offset by the amount of material to process when very large amounts are involved.

“Bulk” is not specifically defined but would be something like at least the volume of a trash bag processed in a session.



# Type III A

Shredders: 2 mm x 15 mm

Disintegrators: based on screen size  
Not greater than 10 mm

# Type IIIB

Shredders: 6 mm x 50 mm

Disintegrators: based on screen size  
max 13 mm dia

**Table 1: Approved Office Category Paper Shredders and Disintegrators Selection Guide**

Classification		Type	Shred Size (Maximum)	Disintegrator Screen Size See Note 3.	Comments
<b>Protected B</b> (where a TRA recommends the use of approved equipment)	General office use	Type IIIA	2mm x 15mm	10mm	See note 1. Type IIIB equipment is approved for bulk destruction only and must not be used for periodic destruction.
	Bulk destruction	Type IIIB	6mm x 50mm	13mm	
<b>Protected C</b>	General office use	Type II	1mm x 14.3mm	6mm	Select Type II (level 6) equipment where a TRA recommends
<b>Confidential</b>	General office use	Type IIIA	2mm x 15mm	10mm	Type IIIB equipment is approved for bulk destruction only and must not be used for periodic destruction.
	Bulk destruction	Type IIIB	6mm x 50mm	13mm	
<b>Secret</b>	General office use	Type II	1mm x 14.3mm	6mm	Select Type II (level 6) equipment where a TRA recommends
<b>Top Secret</b>					

# SEG – Destruction Guide

## Layout

- **Section 1 General Destruction Information**  
overview, limitations and applications and general information;
- **Section 2 Destruction Equipment Selection**  
(paper and text based media) – selection table;
- **Section 3 Destruction Equipment Selection (IT Media)**  
selection tables;
- **Section 4 Commercial Destruction Services**  
guide to the use of commercial fixed facility and mobile destruction services; and
- **Section 5 Incineration – application guidance.**

G1-001



Royal Canadian  
Mounted Police

Gendarmerie royale  
du Canada

Canada

<a href="#">Français</a>	<a href="#">Contact Us</a>	<a href="#">Help</a>	<a href="#">Search</a>	<a href="#">Canada Site</a>
<a href="#">Home Page</a>	<a href="#">Equipment</a>	<a href="#">Guide</a>	<a href="#">Glossary</a>	<a href="#">News</a>



## Security Equipment Guide

This guide was developed to provide security staff and office managers in government institutions with practical advice on physical security equipment and measures required for the protection of assets.

- ▶ [Home Page](#)
- ▶ [Storage](#)
- ▶ [Destruction](#)
- ▶ [Transport & Transmittal](#)
- ▶ [Guide](#)
- ▶ [News and Bulletins](#)
- ▶ [Glossary](#)
- ▶ [Links](#)
- ▶ [Procurement](#)
- ▶ [Custom Testing](#)
- ▶ [Classified Ads](#)
- ▶ [Contact Us](#)
- ▶ [TSB Home](#)

### STORAGE

Equipment List

### DESTRUCTION

Select...

- Select...
- Equipment List
- Equipment Archive
- Selection Guide: Introduction
- Selection Guide: General Information
- Selection Guide: Paper and text based media
- Selection Guide: IT media
- Selection Guide: Destruction Services
- Selection Guide: Incineration

### What's New

July 10, 2007  
[Recent Changes to the Security Equipment Guide News](#)

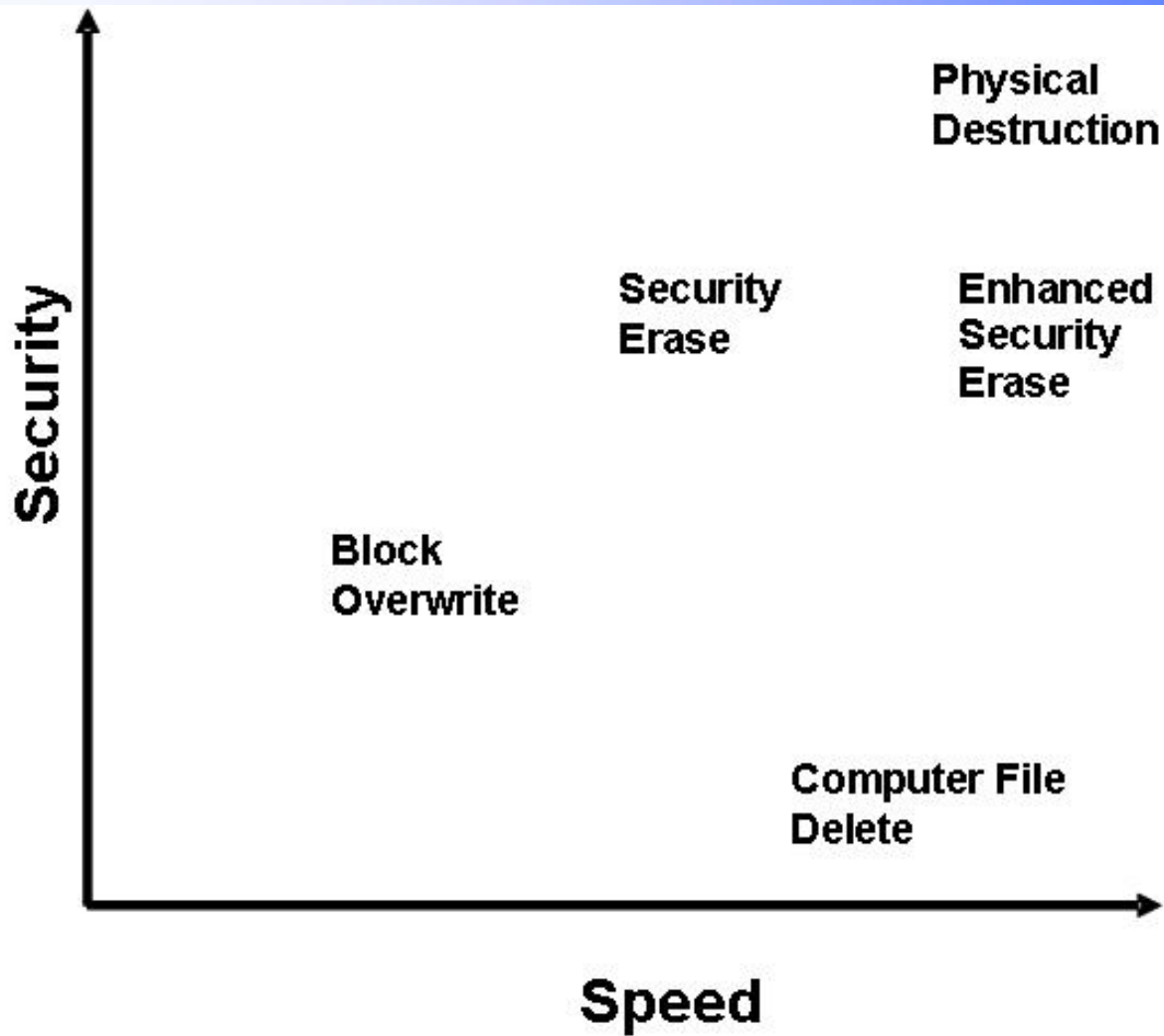
January 2007  
[Revisions to Destruction Equipment Section News](#)

SEG-B1  
[Security Advisory on Key Bumping Bulletins](#)

[More News...](#)

## **Section 3: Destruction of IT Media – Selection Guide**

- Selection of destruction equipment for IT media must take into consideration the medium (e.g.: CD, DVD, hard drive, etc) and security level of the information, as well as the threat and other considerations such as throughput rate, noise and dust generation.
- Normally, it is sufficient to select appropriate destruction equipment from the SEG approved equipment lists for the medium and security level required. For IT media however, it is often necessary to perform other actions such as data over-writes before destruction.



From IEEE Whitepaper on IT Sanitization, 2007

	<b>Shredding, Disintegrating and Grinding Destruction Standards</b>	<b>Destruction Products</b>
<b>Unclas , PA, PB</b>	<i>Disks:</i> at least 3 pieces, each maximum area < 580 mm <sup>2</sup> (e.g., 3x3"). <i>Magnetic tape:</i> pieces, each maximum length < 50 mm (2"). <i>Stripe cards:</i> pieces, each maximum area < 160 mm <sup>2</sup> (e.g., 1/2x1/2").	RCMP Security Equipment Guide (SEG). <i>Note: triple overwrite may be used to downgrade Top Secret media (for subsequent disintegration or shredding as for Secret).</i>
<b>Conf, PC, Secret</b>	<i>Disks:</i> at least 3 pieces, each maximum area < 40 mm <sup>2</sup> (e.g., 1/4x1/4"). <i>Magnetic tape:</i> pieces, each maximum length < 6 mm (1/4"). <i>Stripe cards:</i> pieces, each maximum area < 10 mm <sup>2</sup> (e.g., 1/8x1/8").	
<b>Top Secret</b>	<i>Disks:</i> at least 3 pieces, each maximum area < 10 mm <sup>2</sup> I (e.g., 1/8x1/8"). <i>Magnetic tape:</i> pieces, each maximum length < 3 mm (1/8"). <i>Stripe cards:</i> pieces, each maximum area < 10 mm <sup>2</sup> (e.g., 1/8x1/8").	
	<b>Incineration</b>	<b>Incinerators</b>
<b>All Levels</b>	Total destruction.	Facilities approved by Environment Canada for mixed plastics, etc.
	<b>Emergency Destruction</b>	<b>Destruction Tools</b>
<b>All Levels</b>	Refer to the Annex on Emergency Destruction.	Focused high-impact tool, vise, sledgehammer, etc.
	<b>Degaussing</b>	<b>Degaussing Products</b>
<b>All Levels</b>	Match the degausser power rating to the actual coercivity rating of the media, and carefully follow the degausser product manufacturer directions. Hard drive: insert in degausser chamber and degauss, then turn it around in the chamber and degauss a second time.	Degausser must be CSE-approved for coercivity of the specific media.

## **Section 4: Commercial Destruction Services**

- The security requirements pertaining to commercial destruction services apply to more than just the size of the particle; they apply to the entire process for the destruction of information and include everything from procedures for handling and storing the information to procedures for disposing of the waste, and the facility and its personnel.

# Operational Security Standard on Physical Security

## 10.1 Storage of Protected and Classified Waste

**Protected and classified assets awaiting destruction (either on- or off-site) must be stored at minimum in approved security containers or appropriate secure room as per Appendix B.**

**Departments must safeguard information in transit to destruction, in the manner prescribed for the highest level of classified or protected information involved (refer to RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets)**

## **Destruction Services – Security Aspects to Consider**

- The safeguarding of classified and protected information is a departmental responsibility and “Certificates of destruction” from commercial destruction service providers cannot replace departmental oversight and assurance of destruction.
- Security Requirement Checklist (SRCL) should accompany every destruction contract requisition.
- CISD maintains templates and provides assistance to departments with the preparation of SRCLs.

**CISD**

**Canadian Industrial Security Directorate**

Part of

**Public Works and Government Services Canada (PWGSC)**

# Storage

Classified and protected information should never be stored, even temporarily, at commercial destruction facilities unless the facility has a CISD approved Document Safeguarding Capability (DSC) **that has been issued specifically for temporary storage of documents pending destruction.**

# Temporary Storage and Collection Containers

Containers provided by commercial destruction companies for the collection and/ or temporary storage of documents awaiting collection rarely meet the storage requirements of the GSP.

Containers with open slots are not approved and should never be used for the temporary storage of classified or sensitive information.

Open slot containers may be used for collection and transportation to the destruction site provided they are not used as storage containers and are never left unattended.

- TSB is working with manufacturers and destruction providers to improve their collection box designs to the point that we could accept the associated risks for their use with certain levels of information
  - Unclassified and Protected A
  - Protected B - with Departmental Security Officer acceptance (subject to a TRA)
  - Never for Classified Information

# Mobile Destruction Services

- The following issues are especially relevant to mobile shredder services:
- Location of the Vehicle: Information should be destroyed as close to the origin as possible and preferably, within a controlled and isolated area. Public streets and lanes should never be allowed for classified and highly sensitive information destruction.
- Security clearances: security clearances are rarely given to individual employees of mobile shredding companies due to the instability of this workforce and the difficulties in keeping the clearances current...this is an industry with a high turnover rate of relatively low paid employees.

- Some government departments do not permit the use of mobile shredding services – period. All departments have the responsibility and authority to determine their own policies over and above the base-line standards.
- Some PWGSC Standing Offers permit mobile shredders, but only for Unclassified or Protected A information.
- The GSP requirements are interpreted by some departmental security authorities as prohibiting the removal of Classified material from the department premises until destroyed by approved method/equipment.

# Facility Clearances

CISD performs a facility clearance in accordance with the requirements of the SRCL, which is normally written by the client department. The SRCL is intended to ensure that the facility – as well as transport, handling and storage when part of the contract – is sufficient to ensure the security of protected and classified assets and valuables until destroyed.

# ...Facility Clearances

The CISD Industrial Security Operations Division provides assistance and templates for SRCLs.

Contact:

Canadian Industrial Security Directorate (CISD)  
Public Works and Government Services Canada  
Industrial Security Operations Division  
613-948-4176 (in the NCR)

Questions?