G20-01

Tier 1 Restricted Components Security and Key Control Plan Guideline

Explosives Regulatory Division

June 2022

Canada

Table of Contents

1. Introduction

This guideline is intended to help component seller and product sellers of Tier 1 restricted components develop a security plan for their site. As part of the application to enroll as a seller of Tier 1 components, a declaration must be made that a security plan has been implemented for each location where Tier 1 components will be sold or stored.

The purpose of a security plan is to enhance and maintain the security of a Tier 1 component seller's operation. This is achieved by assessing a site for security risks, developing measures to address security issues and incorporating current security programs into the plan. This plan should formalize responses to security incidents. The plan will also assign people (or positions) within a company to implement specific portions of the plan.

This guideline will also help sellers of Tier 1 components develop a key control plan for their site. As part of the security measures in place, a key control plan must be prepared in writing and implemented (473 (2)). The key control plan can be a separate document or it can be merged with the Security Plan.

The section numbers used in this document refer to the relevant sections under the *Explosives Regulations, 2013 (ER, 2013)*.

There is no specific format for the security and key control plan; however, the listed requirements below must be included. For an example of a Tier 1 Restricted Component Security and Key Control plan, contact the Explosives Regulatory Division and request guideline G20-02.

2. Contents of a Security Plan

2.1 Seller Information

A security plan must be submitted for each location where a seller stores or sells Tier 1 components. The security plan is site specific and the seller information section identifies the company, the specific site, and a person responsible for the security plan at that site. The information that should be contained in this section is identified below:

- Company identification;
- Site identification; and,
- The person responsible for the security plan at the site.

2.2 Emergency Procedures to Address Security Risks

This section of the security plan provides or references the emergency procedures to be followed in responding to the risks identified, and should include assigning a person (or job title of the person) responsible for carrying out the emergency procedures.

An assessment of the security threats is designed to look at a specific site, determine vulnerabilities, and develop effective procedures to address these threats. Some of the scenarios may have a higher risk than others; however, appropriate responses need to be developed for all scenarios considered. Recognizing a potential threat is one of the most effective ways of dealing with it.
Consideration needs to be given to vulnerability to theft, sabotage and unauthorized access by staff, contractors, visitors or outsiders, and dealing with unexplained losses. New and/or existing measures should be described or referenced and a copy should be provided with the plan.

When an emergency response plan covering Tier 1 components is already in place, there is no need to duplicate it in the Security Plan; however, a reference to the emergency response plan must be made. The seller must also ensure to review the emergency response plan to verify that all the requirements listed in this guideline are covered.

2.2.1 Controlling Access to Tier 1 components

Measures must be in place to control access to the Tier 1 component storage area and sales records. These procedures should address unauthorized personnel gaining access to the Tier 1 components or the sales records during all hours, and may include:

- Those that need to be on site (contractors, visitors, unauthorized employees); and,
- Those who are on site surreptitiously (trespassers).

Mechanisms for access control may include fencing, locks, security systems, or other means of preventing access to the product or the sales records.

The access control measures must be described in the Security Plan or reference must be made to the appropriate procedures, and a copy of the procedures must be included with the plan.

2.2.2 Managing Stocks of Tier 1 components

A stock management system must be put in place and a weekly inventory must be conducted and documented (s. 478(1)(3)). A stock management system allows a seller to know the quantity of Tier 1 components currently on hand and allows stock to be reconciled against sales or use. A procedure for dealing with losses must also be developed. As part of the management system, a person or job title of the person responsible for conducting the weekly inventory must be included.

The records may also be used to assist in the annual inventory report required by Natural Resources Canada (s. 479).

The stock management measures must be described in the security plan; or reference must be made to the appropriate procedures, and a copy of the procedures must be included with the plan.

2.2.3 Refusal to Sell

Procedures must be developed and employees must be trained in recognizing conditions that could lead to the refusal of sales (s. 487). If the quantity of a Tier 1 component requested by a buyer is not proportional to their needs and/or it is suspected that the Tier 1 component might be used for criminal purposes, the sale must be refused (s. 481 (1)). If the buyer does not provide sufficient information as per record of sale requirements, the sale must be refused. Other factors that will affect scrutiny of a Tier 1 component sales may include: method of payment, if the customer is new, and/or customer's experience with using a Tier 1 component for legitimate purposes. Procedures to determine need or to assess potential sales to new customers must be developed and employees must be trained in their use.

The refusal of sale measures must be described in the security plan or reference must be made to the appropriate procedure, and a copy of the procedure must be included with the plan.

See G20-04 – Guidelines for Recognizing and Reporting Suspicious Transactions of Explosives Precursor Chemicals for more detailed information.

2.2.4 Reporting Incidents

If any theft, attempted theft, or tampering with a Tier 1 component is discovered, or there is a refusal to sell, it must be reported to:

- The local police or the RCMP National Security Information Network immediately; and,
- The Chief Inspector of Explosives within 24 hours:
  - Phone: **1-855-912-0012**
  - Email: precursors-precurseurs@nrcan-rncan.gc.ca

3. Contents of the Key Control Plan

In order to minimize unauthorized entry, access to a Tier 1 component must be limited by key control through procedures and restricted keyways.

Note: Keys can be under the form of electronic access codes, combinations, access cards or physical keys.

3.1 Authorized Personnel

The plan must include the names of the persons permitted to have access to the keys.

3.2 Management of Keys

Should employees leave the company, or if there are new hires, consideration should be taken as to how keys are accounted for. Keys/locks should be changed, as appropriate.

3.3 Lost, Stolen or Misplaced Keys

If a key is lost or stolen, the lock must be replaced immediately. The plan must detail the process to follow when keys are lost, stolen, or misplaced and when a lock must be replaced.

3.4 Other Considerations

Other aspects should be considered when developing a key control plan:

- If keys are numbered, ensure to keep an updated list of the keys in use (*Note*: the key number must not be marked on the corresponding lock);
- If the keys are kept in a location other than on the employees (e.g locked key box, etc.), indicate where the keys are kept;
- If keys are not in use, employees should ensure they are kept in a secure location.

4. Additional Regulatory Requirements

There are additional regulatory requirements a Tier 1 component seller must follow in dealing with access, control, and reporting. It is a recommendation that the requirements below be discussed in the security plan:

- The local police force must be informed in writing of all locations where a Tier 1 component is to be stored or sold (s. 472);
- All doors, windows, or other access points where a Tier 1 component is stored must be locked when not attended (s. 473 (1));
- All main entrances to a building in which a Tier 1 component is stored must be lit at all times outside business hours (s. 473 (3));
- A sign must be posted at each entrance to a Tier 1 component storage area warning against unauthorized access (s. 475 (1));
- Access to a Tier 1 component storage area and sales records must be limited to persons authorized by the seller (s. 475 (2), 484 (3));
- A list of all employees who work at each location where a Tier 1 component is stored or sold must be kept (s. 476);

- Procedures should be put in place for the verification upon receiving a Tier 1 component shipment (s. 477), the identification of buyers (s. 482), and the completion of a record of sale (s. 484);

5. Confidentiality and Review

5.1 Confidentiality

The security and key control plan should be treated as a security-sensitive document. The seller should limit and control its distribution and ensure that the original and approved copies of the plan are stored in a secure location.

5.2 Update of the Security Plan

The Security Plan must be updated every 12 months (s. 474).

5.3 Employee Training

Training should be offered to employees regularly to ensure they are familiar with the plan/updated plan and its procedures and their responsibilities to report incidents related to a Tier 1 component.