SIPI Chicago

Site Security Target

Rev. 1.6 — 5 June 2024 Evaluation document
NXPOMS-1719007347-16618 PUBLIC

Document information

Information	Content
Keywords	Common Criteria, Destruction Site, SIPI Metals Corporation, U.S., Site Security Target
Abstract	Site Security Target for the site certification of the site SIPI Metals Corporation, Chicago, Illinois, United States of America

1 Document Information

1.1 Reference

Title:	SIPI Chicago - Site Security Target
Version:	1.6
Date:	5 June 2024
Company:	SIPI Metals Corporation
Name of the site:	SIPI Metals Corporation
Site Type:	Secure Destruction
EAL:	EAL: SARs taken from EAL6

1.2 Revision History

Rev.	Date	Description	Author	Owner
1.0	2020-06-25	Initial version of the document, created first Version by NXP DITA Oxygen XML Template.	Gordon Caffrey	Gordon Caffrey
1.1	2020-06-29	SIPI specific information added. Reduced scope to reflect site services.	Gordon Caffrey	Gordon Caffrey
1.2	2020-07-13	Update after AST comments from Brightsight.	Gordon Caffrey	Gordon Caffrey
1.3	2020-09-11	Update after additional comments.	Gordon Caffrey	Gordon Caffrey
1.4	2022-04-21	Switch to final version of NXP DITA Oxygen XML Template. Adding service S.Incoming_Shipment.	David Herrgesell	David Herrgesell
1.5	2022-06-22	Update based on certifier comments	David Herrgesell	David Herrgesell
1.6	2024-06-05	Update after internal review	David Herrgesell	David Herrgesell

2 SST Introduction

This document is based on the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site.

This Site Security Target is intended to be used by only one specific client, namely NXP Semiconductors B.V.. Therefore, the term 'client' in this document refers directly to NXP Semiconductors B.V..

In the following chapters you will find several times statements like 'this and/or that'. The applicability is given by the 'type of site' and the definition of assets.

2.1 Identification of the Site

The site SIPI Metals Corporation is located at:

```
1720 N. Elston Avenue
Chicago, Illinois 60642-1579
United States
www.sipicorp.com
```

2.2 Site Description

2.2.1 Physical Scope

The entire building and the surrounding fenced area specified in Section 2.1 are in the scope of this SST. The surroundings of the fenced area are not in scope of this SST, hence the fence surrounding the building is forming the physical boundary of the site.

2.2.2 Logical Scope

The following life-cycle phases as defined in 'Security IC Platform Protection Profile with Augmentation Packages' (PP-0084) are subject of the SST:

- Phase I: IC Embedded Software Development
- Phase II: IC Development
- Phase III: IC Manufacturing
- Phase IV: IC Packaging
- Phase V: Composite Product Integration
- Phase VI: Personalisation
- Phase VII: Operational Usage

Note that destruction of security items can happen during any of the life-cycle phases defined in PP0084. Even during Phases V, VI and VII, where security items could be sent back to the client from the composite product integrator, or end-users of the TOE.

The site is solely used for secure destruction of NXP assets, and no sensitive, logical information is transferred between the site and NXP.

2.2.3 List of services in Scope

The following service(s) and/or processe(s) provided by the site (is) are in the scope of the site evaluation process. Some processes are directly part of the phases presented before and others are supporting processes which can be involved at any phase of the development. The services are detailed in section Section 8.2.

S.Incoming_Shipment

S.Scrapping

3 Conformance Claim

The SST is conformant to Common Criteria Version 3.1 ([3], [4]).

For the evaluation the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1 ([5])

The evaluation of the site comprises the following assurance components:

- **ALC_DVS.2**
- **ALC_LCD.1**

The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile [2] and is therefore suitable for the evaluation of (software for) Security ICs.

The chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-Cycle Support". For the assessment of the security measures attackers with a high attack potential are assumed. Therefore, this site supports product evaluations up to EAL6.

4 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of the TOE and the security management of the site.

4.1 Assets

Depending on the setup of the Site, the protection of the following assets is needed:

Physical Security Objects: The site has physical security objects in relation to the "intended TOEs". Both the integrity and the confidentiality of these must be protected.

- Data Storage
  - Inactive but accessible unencrypted data
  - Defect but holding unencrypted data
- Samples
- Photomasks (good and fail/broken parts)
- Wafers and dies (all processing states, all treatment steps, good and fail parts)
- Scrap material
- Probe cards
- Probe card and load board
- Modules or other packages (good and fail parts)
- Finished products (good and fail parts)
- Security Seal Tape
- IT Infrastructure (e.g. VPN, Switches, network components)
- Customer returned samples (all processing states, all assembly steps, good and fail parts)

Site Certification Data: The site has access to documentation needed to successfully pass a site certification. Both the integrity and the confidentiality of this data must be protected.

- SIPI Procedure #5794: NXP - Secure Destruction
- SIPI Security Procedures and Protocol

4.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Rugged-Theft: An experienced thief with specialised equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive assets.

T.Unauthorised-Staff: Unauthorised employees or subcontractors get access to assets or systems used for development, configuration management and/or production, so that the confidentiality and/or the integrity of the "intended TOE" is violated. This can apply to any development and/or production step and any asset related to the "intended TOE" or its configuration.

T.Staff-Collusion: An attacker tries to get access to assets handled at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

T.Attack-Transport: An attacker might try to get hold of any assets during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the assets during the shipment/delivery process to allow a modification, cloning or the direct/indirect retrieval of confidential information.

4.3 Organisational Security Policies

P.Reception-Control: The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the client. Furthermore, it is verified that the "intended TOE" can be identified and a released process is defined for the "intended TOE". If applicable this aspect includes the check that all required information and data is available to handle the incoming items.

P.Product-Transport: Technical and organisational measures ensure the correct labelling of the "intended TOE". A controlled internal shipment and/or the external delivery is applied. The transport supports traceability up to the recipient. If applicable or required, this policy includes measures for packing to protect the product during transport.

4.4 Assumptions

Each site operating in a production flow must rely on preconditions provided by the previous site. Each site must rely on the information received by the previous site/client. This is reflected by the assumptions that must be defined for the interface.

A.Item-Identification: For the processing of NXP material the client shall provide information which can uniquely identify the delivered packages.

5 Security Objectives

The Security Objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal shipment and/or the external delivery.

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the "need to know" principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The site enforces two or three levels of access control to sensitive areas of the site. The access control measures ensure that only registered and authorized people can access restricted areas. Sensitive products and data are handled in restricted areas only. Network cabling is protected according to classification of the transferred data by avoiding routes through public areas or by usage of appropriate cryptographic measures.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

O.Alarm-Response: The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any sensitive configuration item (assets). After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

O.Internal-Monitor: The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.

O.Maintain-Security: Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

O.Staff-Engagement: All employees who have access to sensitive configuration items and who can move parts of the product out of the defined production/development flow are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job.

O.Reception-Control: Upon reception of any material an immediate incoming inspection is performed on the packaging with the delivery weight confirmed. The total inspection comprises confirming the delivery weight, the received amount of material, their package identification, and the assignment of the items to a related internal process.

O.Incoming-Shipment: The security items that shall be destroyed are shipped according the defined secure shipment process, where the packaging is part of that agreed process between client and the site. The shipment method assures integrity and confidentiality of the physical security items during transport from the client to the site.

The shipping service provider supports tracing of the security items to be destroyed during the shipment.

5.1 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are pre-conditions fulfilled either by the site providing the sensitive configuration items or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

5.1.1 Mapping of Security Objectives

All the given security objective(s) in the table below counter(s) the threat / OSP.

Table 1. Security Problem Definition mapping to Security Objective

Security Problem Definition / Threats	Security Objective
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Staff-Engagement
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement
T.Attack-Transport	O.Reception-Control
Security Problem Definition / Policies	**Security Objective**
P.Reception-Control	O.Reception-Control
P.Product-Transport	O.Incoming-Shipment

5.1.2 Objectives Rationale

The following rationale provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

O.Physical-Access: The site implements a "need to know" principle by separation measures using a combination of physical partitioning together with technical and organisational security measures. The access control measures support the enforcement of the separation and the "need to know" principle. The handling of assets is restricted to separate security areas.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Security-Control: The site is using dedicated, trained security personnel for guard services. These personnel are responsible for operation of the access control and alarm systems, performing patrol rounds, visitor registration, physical key management, the surveillance of the technical alarm sensors and the responses to incidents.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Alarm-Response: In case of an access attempt to an asset by an unauthorized person, the site has an alarm system in place. After the alarm is triggered the unauthorised person still must overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Internal-Monitor: Regular meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This includes the assessment of security alarms and associated logs of the physical and logical protection. In addition, results of internal audits and assessments are reviewed.

This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion.

O.Maintain-Security: The security related surveillance and alarm systems are maintained on a regular basis. The physical and logical access permission are reviewed and updated if needed. Logs of the associated systems are reviewed to support the work.

This helps to prevent the threat(s) T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion.

O.Staff-Engagement: The site has established personnel security measures. All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. This provides legal liability to protect the assets against disclosure. Furthermore, all employees are qualified for their job, are trained and had to pass a questionnaire to check the security awareness.

This helps to prevent the threat(s) T.Unauthorised-Staff and T.Staff-Collusion.

O.Reception-Control: When design/test/production data is received, the integrity and completeness of the data is verified and assigned to the related client order. The link between data and client order ensures the unique identification. When receiving physical assets, an inspection of the items is performed in order to acknowledge the correct amount, their identification and the assignment. Received assets are registered within the tracking system.

This helps to address the OSP(s) P.Reception-Control .

O.Incoming-Shipment: Packing procedures including seal tape and the tracking of the transport support the identification of manipulations during the transport. The address of the client is part of the product setup and included in the requirements specification of the client.

This directly addresses the OSP P.Product-Transport. The threat T.Attack-Transport can be prevented.

6 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

7 Security Assurance Requirements

Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [2].

The Security Assurance Requirements (SAR) are:

- Development Security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

The Security Assurance Requirements listed above fulfil the requirements of [6] because hierarchically higher components than the defined minimum site requirements (ALC_DVS.1) are used in this Site Security Target.

In addition, the minimum set of SARs is extended by SAR of the assurance components for "Life-cycle definition" (ALC_LCD.1), .

The dependencies for the assurance requirements are as follows

- ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- ALC_CMS.5: None
- ALC_DEL.1: None
- ALC_DVS.2: None
- ALC_LCD.1: None
- ALC_TAT.3: ADV_IMP.1

7.1 Application Notes and Refinements

The description of the site certification process [6] includes specific application notes. The main item is that a product that is considered as "intended TOE" is not available during the evaluation. Since the term "TOE" is not applicable in the Site Security Target, the associated processes for the handling of products, or "intended TOEs" are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

The SST in hand has been refined to consider "intended TOEs" rather than specific TOEs. All other refinements as stipulated by the corresponding subsections in "Application Notes for Site Certification" [6], chapter 5 of the chosen Assurance Classes have been applied as well. In addition, the relevant refinements of the Eurosmart PP [2] have been considered.

7.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [4] to the Security Objectives defined in this SST. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, this process is based on the assumption that the received configuration items are appropriately labelled and identified.

Note: The content elements that are changed from the original CEM [5] according to the application notes in the process description [6] are written in italic. The term TOE can be replaced by "configuration items" in most cases. In specific cases it is replaced by "intended TOE". "Configuration items" is used here in the sense that these are items contributing to build or to produce the TOE.

The SAR Rationale does not explicitly address the developer action elements defined in [4] because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. This includes the requirement that the procedures are applied as written and explained in the documentation.

7.2.1 Rationales, Aspects and References for ALC_DVS.2

ALC_DVS.2.1C - The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *intended* TOE design and implementation in its development environment.

Security Objective	Rational
O.Physical-Access	This covers the physical measures.
O.Security-Control	This covers the organizational measures of the guard team.
O.Alarm-Response	This covers the physical measures and their alarm follow up by the guard team.
O.Internal-Monitor	This covers organizational measures by reviews and management attention.
O.Maintain-Security	This covers organizational measures by maintenance.
O.Incoming-Shipment	This covers procedural measures regarding transport of security items for destruction.
O.Staff-Engagement	This covers personnel measures.

Aspects	Reference
- Access control to development areas inside the building, surveillance, alarm system and guard services to prevent access to the security area for unauthorized persons - Operation of the physical security system, emergency procedures, incident handling and reporting - Tracing and control of Visitors, external suppliers and cleaning personnel - Internal storage of products in a strong room, handling of physical objects, zero balancing, disposal of security products - Trustworthiness and training of staff	- SIPI Procedure #5794: NXP - Secure Destruction, Revision C, April 14 2022

Aspects	Reference
- Organizational measures to enforce security and alarm tracing - Personal accountability for products - Policies and procedures for the internal handling of confidential information - Network security measures to ensure logical protection and authentication to computer systems using username and password - Maintenance of security measures - Protection of the internal shipment - Destruction of sensitive documents, data, products and other items	

ALC_DVS.2.2C - The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *intended* TOE.

Aspects	Reference
The justification is provided in this site security target because it shows that all threats are addressed by the measures. In addition, the measures are monitored to control the effectiveness. Besides this the lifecycle documentation also provides a justification from a different angle.	- This SST, see chapter 7.2 Security Assurance Rationale

The security assurance requirements of the assurance class "Development security" listed above are required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during development, production, testing, assembly and pre-personalization or personalization of the "intended TOE" can be used by potential attackers for the development of attacks. Any keys loaded into the "intended TOE" also support the security during the internal shipment or the external delivery. Therefore, the handling and storage of electronic keys must also be protected. Further on the Protection Profile [2] requires this protection for sites involved in the lifecycle of Security ICs development and production.

7.2.2 Rationales, Aspects and References for ALC_LCD.1

ALC_LCD.1.1C - The life-cycle definition documentation shall describe the model used to develop and maintain the *intended* TOE.

Aspects	Reference
The "intended TOE" is developed and maintained as per the life-cycle definition in Protection Profile PP0084 [2] .	Protection Profile PP0084 [2]

ALC_LCD.1.2C - The life-cycle model shall provide for the necessary control over the development and maintenance of the *intended* TOE.

Aspects	Reference
The applied processes provide the necessary controls over development and maintenance of the "intended TOE".	- SIPI Procedure #5794: NXP - Secure Destruction, Revision C, April 14 2022

The security assurance requirements of the assurance class "Life-cycle definition" listed above are suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. One site provides only a limited support of the described lifecycle for the development and production of Security ICs. However, the assurance requirements are suitable to support the application of the site evaluation results for the evaluation of an "intended TOE".

8 Site Summary Specification

Please refer for the rationales, aspects and references to the subchapters in Section 7.2 for the different ALC classes.

8.1 Preconditions Required by the Site

This section includes justifications for the assumptions defined in the SST. These assumptions are relevant for the splicing process since they must be examined during the product evaluation. Especially aspects like the classification of items and the appropriate provision of specifications for the site must be verified by checking appropriate evidence (e.g. the set of specifications provided to the site with a site certificate) during the product evaluation.

The following table explains the preconditions of the client that are required to ensure the security measures of the site in order to protect its assets.

Table 2. Preconditions of Assumptions

Assumption	Precondition
A.Item-Identification	Before sending items to this site, the previous site must label it uniquely. Those unique identifiers can come from the client's configuration management system.

8.2 Services of the Site

Table 3. Services of the Site

Service of the Site	Explanation of the Service
S.Incoming_Shipment	This site provides a secure shipment service for items that shall be destroyed on the site according the defined secure destruction process. The shipment methods assures integrity and confidentiality during transport of the physical security items from the client to the site. *Assumptions:* **A.Item-Identification** must be fulfilled.
S.Scrapping	This site provides a scrapping service for other sites having a business relationship with NXP, to hand in defect or rejected security items (e.g. finished, semi-finished, wafers, hard discs containing unencrytped data) which are destroyed according to the defined secure destruction process. *Assumptions:* **A.Item-Identification** must be fulfilled.

9 Bibliography

[1] Eurosmart. Site Security Target Template, Version 2.0, 15. April 2021.

[2] Eurosmart. Security IC Platform Protection Profile with Augmented Packages (BSI-CC-PP-0084-2014), Version 1.0, 2014.

[3] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[4] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017.

[5] Common Criteria. Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[6] Common Criteria. Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007.

10 Glossary

CA – Certificate Authority

CC – Common Criteria

CCC&S – Competence Center Crypto & Security

CI – Configuration Item

CKC – Customer Key Creation (system for key creation and post-shipment services)

CL – Configuration List

CM – Configuration Management

CSH – China Secure High Confidential

CSM – China Secure Main Confidential

CSR – Certificate Signing Requests

CTO – Chief Technology Organization

CSx – China Secure - Main or High Confidential

DDS – Data Delivery Service

DiT – Data Intake and Translation

DIT – Data Intake

DMZ – Demilitarized Zone

DNV – Dynamic Non-volatile

EAL – Evaluation Assurance Level

FH – Fabkey Helpdesk (old name of DNV desk)

FS – Facility Secure

FAE – Field Application Engineer

HS – High Secure

HSM – Hardware Security Module

IC – Integrated Circuit

IP – Intellectual Property

KDS – Key Delivery Services

KIS – Key Insertion Server

MBK – Master Backup Key

NPIT – New Product Introduction Team

OEF – Order Entry Form

OSP – Organizational Security Policy

PP – Protection Profile

PS – Production Secure

PS-HS – Production Secure-High Secure

PS-RS – Production Secure-Restricted Secure

PMP – Project Management Plan

PQE – Product Quality Engineer

RCS – ROM Code System

ROM – Read-Only Memory

RS – Restricted Secure

SAR – Security Assurance Requirement

SNV – Static Non-Volatile

SNR – Serial Number Server

SSM – Site Security Manual

SST – Site Security Target

ST – Security Target

TOE – Target of Evaluation

TP – Trust Provisioning

TSM – Trusted Service Manager

Tables

SIPI Chicago

Site Security Target

Contents

Date of release: 5 June 2024
Document number: NXPOMS-1719007347-16618