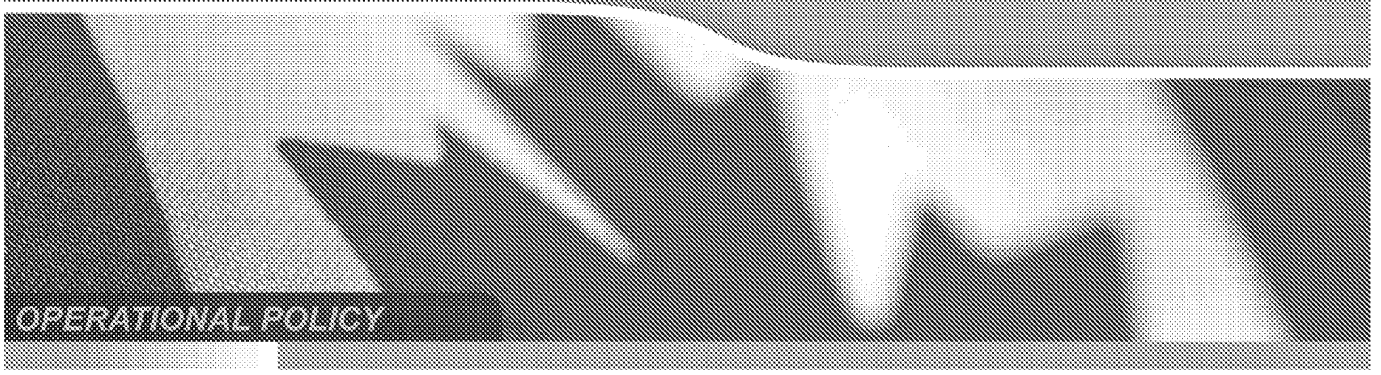
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

OPS-1-7

Operational Procedures for Naming in SIGINT Reports



Canada

Table of Contents

1. Introduction

Policy Scope and Application

1.1 Scope

These procedures govern the process for including a Canadian or Second Party (defined as citizens or permanent residents, corporations and organizations of Second Party nations) identity in:

- SIGINT reports issued under "part (a)" of the CSEC mandate, and

IRRELEVANT

This document supersedes OPS-1-7, *SIGINT Naming Procedures,* dated 2 September 2005.

1.2 Objective

These procedures provide direction to you and your managers on:

- deciding whether to refer to an identity
- how to suppress an identity
- how to retain an identity in the SIGINT reporting database
- when naming a Canadian or Second Party person, corporation or organization is allowed without requiring senior management approval
- when naming a Canadian or Second Party person, corporation or organization is allowed but you must seek senior management approval
- what to do in case a Canadian or Second Party identity has been accidentally revealed, and
- Second Party naming rules.

1.3 Policy Scope and Application

To comply with the legal authorities governing its activities, it is CSEC policy to protect the privacy of Canadians by suppressing the identities of Canadian persons, corporations and organizations in SIGINT reports, except in the specific circumstances covered in Chapters 4 to 7 of these procedures.

For Second Party identities, it is CSEC policy to honour the naming rules of Second Party partners. For summaries of Second Party naming policies, see Annexes 3 to 6.

CSEC's reporting programs are subject to
- internal monitoring for policy compliance, and
- external audit and review by various government review bodies, including, but not limited to, the CSE Commissioner and the Privacy Commissioner.

1.4 Application

The following staff must read, understand and comply with these procedures:
- CSEC and CFIOG staff, and
- any other parties, including secondees, integrees, and contractors

who are involved in the production and release of reports governed by these procedures.

Activity Description

1.5 What Are Naming Rules?

"Naming rules" protect the privacy of Canadian and Second Party persons, corporations and organizations in SIGINT reports. Naming rules determine whether an identity found in intercepted information may be named in a report, or whether it must be completely suppressed and replaced with a generic term instead.

You must apply these rules when a Canadian or Second Party identity appears in reportable traffic, and you find it necessary to refer to the identity in a report either through naming or suppression. This would happen, for example, if the intelligence makes no sense without the reference, or if the identity is an important component of the foreign intelligence.

Continued on next page

1.5 What Are Naming Rules? (continued)

Note: Throughout these procedures:
- "name" means to fully or partially identify a Canadian or Second Party person, corporation or organization by name or title; for example, "Bob Smith" or "the Canadian Prime Minister".
- "suppress" means to fully mask the identity of a Canadian or Second Party person, corporation or organization, and replace the name with a generic term; for example: "Named Canadian 1".

Legal Framework

1.6 Legal Authorities

Reports issued under part (a)

Paragraph 273.64(1)(a) of the *National Defence Act* (NDA) (part (a) of the CSEC mandate) provides CSEC with the authority to acquire and use information from the Global Information Infrastructure (GII), for the purpose of providing foreign intelligence in accordance with Government of Canada (GC) intelligence priorities.

Paragraphs 273.64(2)(a) and (b) of the NDA direct that CSEC's part (a) activities must not be directed at Canadians or any person in Canada, and must be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information. Privacy measures are also described in the *Privacy Act*, the *Ministerial Directive to CSE on the Privacy of Canadians* and in OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*.

Accordingly, CSEC has measures in place to protect the privacy of Canadians, which include protecting information about Canadians in SIGINT reports.

Information about Canadians is defined as:
- any personal information (as described in the *Privacy Act*) about a Canadian, or
- information about a Canadian corporation.

For the purpose of these procedures, Canadian organizations are accorded the same protection as Canadian citizens and corporations.

Continued on next page

1.6 Legal Authorities (continued)	IRRELEVANT
1.7 Exemption to these Procedures: "Other" Part (c) Reporting	

2. Deciding to Refer to an Identity

Attention: These procedures document the process for naming, not targeting, a Canadian or Second Party identity in SIGINT reports. SIGINT reports must focus on the foreign intelligence conveyed, not on the fact that one end may incidentally be Canadian or Second Party.

2.1 Definition of a Person, Corporation and Organization

The first step in the naming process is to determine whether reportable traffic relates to a Canadian or Second Party person, corporation or organization.

While this may seem intuitive, the terms "person", "corporation" and "organization" have precise definitions that are based in law.

CSEC definitions are as follows:

- **A Canadian person** is a Canadian citizen or permanent resident of Canada located anywhere in the world. A person who is temporarily in Canada on a student, worker or visitor visa, for example, is not a Canadian and may therefore be named (but not targeted).
- **A Canadian corporation** is a business, company, firm, financial institution or other commercial enterprise that is incorporated in Canada either under federal or provincial legislation. This includes any subsidiary of a Canadian corporation which is itself incorporated in Canada. A company must be incorporated in Canada to be considered Canadian. Merely registering a company in Canada does not give it any Canadian status. (See paragraph 4.7 for more details on subsidiaries.)
- **A Canadian organization** is an unincorporated association, for example, a political party, a religious group, or an unincorporated business headquartered in Canada.

Consult Annexes 3 to 6 for guidelines on how Second Parties define their own entities.

2.2 What is an Identity?

As a second step, you must determine if the reportable traffic contains a Canadian or Second Party identity.

An identity is information that can be uniquely associated, directly or indirectly, with a Canadian or Second Party person, corporation or organization. It can include, for example, a name, [redacted] telephone number, e-mail address, IP address, passport number, [redacted]

2.3 To Include an Identity or Not

As a third step, when drafting a report, if you have traffic containing a Canadian or Second Party identity, you must ask yourself whether you actually need to refer to it.

If the identity will not contribute to the use and understanding of the reported intelligence, omit it altogether. Don't refer to an identity simply because it is available.

If, on the other hand, the identity will contribute to the value of the foreign intelligence, then you should refer to it. For example, the reader may need to know the identity to understand or assess the information.

> **Attention:** Never refer to a Canadian or Second Party identity in Write-to-Release (WTR) paragraphs. See OPS-5-3, *Write-to-Release (WTR) Procedures,* for more information.

2.4 Basic Rule for Referring to a Canadian Identity

In the specific circumstances covered in Chapter 4, you may name some Canadian or Second Party people, corporations or organizations without the need for approval.

You may also name a Canadian or Second Party person, corporation or organization if you have obtained approval to:

- contextually identify a Canadian (see Chapter 5), or
- name or forward the identity of a Canadian person in threat-to-life reporting (see Chapter 6) to a restricted group of recipients, or
- name a Canadian person [redacted] (see Chapter 7).

Continued on next page

2.4 Basic Rule for Referring to a Canadian Identity (continued)

Under every other circumstance, you must mask or "suppress" identities of Canadian or Second Party people, corporations or organizations (see Chapter 3).

Attention: When a Canadian identity appears in collateral that is being used in a report, you must replace it with a generic term such as "a Canadian company" or "a Canadian person" unless the identity qualifies for naming (see Chapter 4) and is essential to the understanding of the report. When a Second Party identity appears in collateral that is being used in a report, you must follow the rules of the relevant Second Party.

2.5 Rules for Reporting Second Party Identities

If you want to name a Second Party person, corporation or organization, you must follow the process outlined in the relevant Second Party naming policy. Excerpts from these policies are included in Annexes 3 through 6. You should send questions related to naming issues not covered in the annexes to Operational Policy.

---

3. Suppression Rules

3.1 Generic References

Unless naming is allowed or special approval has been given, you must suppress an identity in a report by replacing it with a generic term so that the identity cannot be deduced by a reader.

The term can be generic, such as "a named Canadian person", or it can be a more descriptive term, such as "a Canadian member of the [redacted] (unless the organization is Canadian or Second Party).

To avoid confusion, you must use the same generic reference for a recurring identity throughout the report.

> **FYI:** Examples of Canadian identities that might appear in traffic and suggested wording in reports are included in Annex 2.

3.2 Unknown Nationality

If the person, corporation or organization is located in Canada or in a Second Party country, you should assume Canadian or Second Party status unless there is firm evidence to the contrary.

Where there is uncertainty as to whether or not an identity is Canadian or Second Party (for example, a target owns property in Canada or a Second Party country), you must use a generic term such as "a possible Canadian person" or "a probable Australian".

3.3 Partially Identified and Unidentified People

If a person is only partially identified in traffic you must use phrases such as "a partially identified Canadian" or "a partially identified UK person".

If you know that a person appearing in traffic is Canadian or Second Party but that person is not named, you must use a phrase such as "a Canadian person (not further identified)" or "an unidentified US person".

3.4 Avoiding Contextual Identification

In some cases, a reader can guess an identity from the report's content even when it has not been included; for example, if the report deals with a Canadian who is being held hostage in a foreign country, and the hostage-taking has been highly publicized. This is called contextual identification.

Contextual identification is equivalent to naming and is therefore only allowed under certain conditions and with senior management approval. See Chapter 5 for details on what to do in the case of a contextual identification.

Retention and Release of Identities

3.5 Marking Identities in the Report Writing Tool

To replace an identity with a generic term when writing a report, you must first type the identity in the report-writing tool, then enter the generic term that will replace the identity in the final product [redacted]

Marking will ensure that the identity is properly stored in CSEC's SIGINT reporting database so that Operational Policy can retrieve it should a client request the identity.

FYI: See CSOI-4-1, *SIGINT Reporting*, for details on how to mark identities for retention when writing reports using the report-writing tool.

3.6 What to Include in the Report Writing Tool

You must only include the essential details about the identity in the report-writing tool. You must not include extraneous information about a Canadian or Second Party entity such as gender, address or position title, unless it adds to the report's foreign intelligence value.

Continued on next page

3.6 What to Include in the Report Writing Tool (continued)

The following table illustrates examples of when to include more than simply the identity of the Canadian (also applicable to Second Party identities).

If the alias used in the report is...	And ...	Then include in "Add Suppressed Identity" feature ...
the name of a Canadian company	the company's president is mentioned in traffic, but is not referred to in the report	only the name of the company
a Canadian terrorist	additional information is included in traffic	all available information (for example, phone number, e-mail address) to assist CSIS and other departments or agencies with valid operational justifications to receive this information

3.7 Release of Suppressed Identities

Access to identities in CSEC's report-writing tool is strictly controlled so that only Operational Policy staff and report actors have access.

Recipients of SIGINT reports containing a suppressed Canadian or Second Party identity, who have an operational requirement to know the unsuppressed identity, must request this information by following the process outlined in OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports.*

Only Operational Policy staff is authorized to release this information in accordance with OPS-1-1. This means, for example, that you must never provide a Canadian or Second Party identity to a CSIS analyst, by any means, including by telephone.

Warning: Anyone outside Operational Policy who releases an identity is committing a privacy violation.

4. When Naming is Allowed

4.1 Permitted Types of Naming

This chapter lists the types of naming that are allowed without the need for approval. Naming includes revealing the full identity of a person, corporation or organization, or partial naming (for example, revealing a person's job title).

Allowing naming does not imply allowing targeting.

> **Note:** Certain information about GC employees is excluded from the definition of personal information in the *Privacy Act*, and so it does not require the same privacy protection measures. The complete definition of what is and is not personal information is included in Annex 1.

4.2 GC Institutions

You may fully name GC institutions, as well as their publications, in SIGINT reports if such identification adds to the foreign intelligence value of the report. This also applies to web addresses (for example, www.canada.gc.ca) and IP addresses that cannot be linked to an individual.

You may also name domain names associated with GC e-mail addresses (that is, the information following the "@" sign of an e-mail address). You must suppress the name before the "@", however (for example, "namedCanadian[redacted]gc.ca"), regardless of the seniority of the individual concerned.

4.3 GC Employees

You may name Federal Ministers in the current Cabinet, acting in their official capacity, and senior federal public servants, acting in their official capacity, by title, but only if such identification is necessary to understand the foreign intelligence or assess its importance.

This table gives some examples (see Annex 2 for additional examples):

Continued on next page

4.3 GC Employees (continued)

Use...	Instead of...
"the Canadian Prime Minister"	"a Canadian official"
[redacted]	

4.4 Exceptions to GC Employees

You must only refer to federal public servants below the level of Director in general terms, for example, [redacted] Refer to officials at [redacted]

4.5 Canadians in International Organizations

You may name Canadians working for international organizations such as the UN, acting in their official capacity, by title, but only if such identification is necessary to understand the foreign intelligence or to assess its importance. You must not indicate in any way that this person is Canadian.

4.6 [redacted]

4.7 Subsidiaries of Canadian Corporations

You may name foreign-incorporated or foreign-registered subsidiaries of Canadian corporations abroad. If a foreign subsidiary and its parent company in Canada are mentioned in the same report, however, you must not name the subsidiary; use generic terms such as "a Canadian company and its [redacted] subsidiary".

4.8 Vessels

You may name vessels owned by the GC, such as Coast Guard or Canadian Forces vessels.

[redacted]

4.9 [redacted]

4.10 Media

Only name a Canadian newspaper, magazine, wire service, radio, or television network when:

- it is being used as a brand name, or
- you are citing factual or statistical information (not editorial opinions) as unclassified collateral.

4.11 Provinces, Cities

Only name Canadian cities, provinces and territories when you are using them as geographic references. Use generic terms such as "a Canadian province" when identities or the political, social or economic agendas of municipal, provincial or territorial people, corporations or organizations may be revealed.

4.12 Geographic Addresses

You may name Canadian addresses used to describe a location (for example, hotels or restaurants) provided the reference is neutral and you identify the Canadian entity only in the context of its primary purpose [redacted]

4.13 Brand Names

You may name products of Canadian companies provided you focus on the use of the product, not the manufacturer of the product (see example 1 below). This permission does not apply if only one company manufactures and sells the product, since naming the product would identify the company (see example 2 below).

Examples

1. [redacted]
2. [redacted]

4.14 [redacted] You may name e-mail or IP addresses [redacted]

5. Contextual Identifications

5.1 What is a Contextual Identification?

A contextual identification occurs when an identity is suppressed but the description of the Canadian or Second Party person, corporation or organization provides enough information for a reasonably informed person (that is, someone who routinely reads a major newspaper, watches TV news, or visits news websites) to be able to guess or research the actual identity.

There are times when avoiding the contextual identification of a Canadian or a Second Party would render a report useless from a foreign intelligence perspective; therefore, if you must include such an identification, senior managers must approve its use before you release the report.

Recognizing and Deciding Whether to Use a Contextual Identification

5.2 Step 1: Determining Whether You Have a Contextual Identification

Recognizing whether a person, corporation or organization is actually being contextually identified is not always easy. You should ask yourself whether the content of the report as a whole would allow an informed reader to identify the suppressed identity. The following example illustrates a possible process for determining whether or not a suppressed identity is actually a contextual identification.

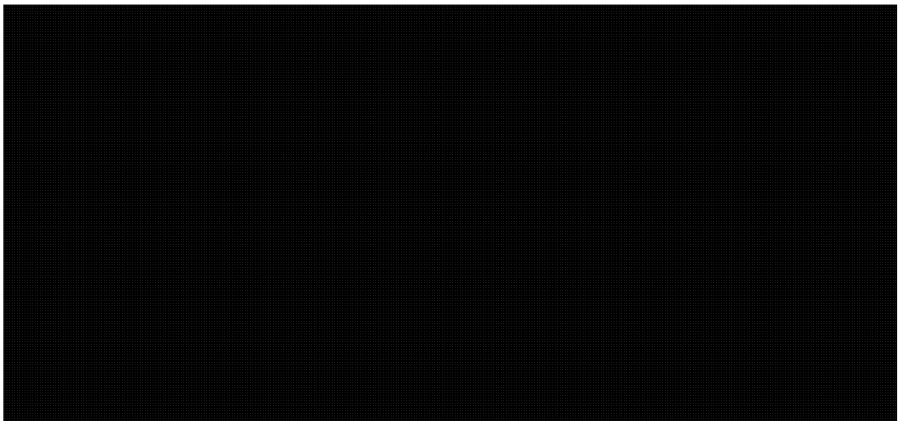
Example:

Q1:

A1:

Q2:

A2:



Continued on next page

5.2 Step 1: Determining Whether You Have a Contextual Identification (continued)

[redacted]

5.3 Step 2: Deciding Whether to Use a Contextual Identification

Before deciding whether to contextually identify a Canadian or Second Party person in a report, you should consider other options. These are

- using a normal suppression phrase such as "a named Canadian person", if there is no doubt as to the identity of the Canadian, and then following the usual steps for including a suppressed identity in a report, or
- making the alias and accompanying information less specific so that multiple people, corporations or organizations might fit the description, thereby making contextual identification no longer possible.

If more than one Canadian person, corporation or organization is planning some activity [redacted], this is not a contextual identification, so you should use a normal suppression phrase.

If neither of these options fits the situation, and if the contextual identification is essential to the foreign intelligence, you should follow the process set out in the following paragraphs for obtaining the necessary approvals.

5.4 Step 3: Deciding On One-Time or Blanket Approvals

You should assess whether the contextual identification is likely to recur in future reporting. If the situation is unlikely to recur, this is a "one time" contextual identification, and you should follow the one-time approval process in paragraphs 5.5 through 5.7.

If, however, you come across a situation that seems likely to be ongoing (for example, [redacted], then you should get a "blanket" approval (which covers a specific time period) for this report and all future reports that contain the same contextual identification. In such a case, follow the blanket approval process in paragraphs 5.8 through 5.13.

Requesting Approval – One Time

5.5 Senior Management Approval

You must obtain senior management approval to include contextual identifications in a report.

- [redacted] or Deputy Chief (DC) SIGINT, or any person designated to act in these positions, must assess the report as part of their OPS-1 report release sign-off responsibilities (see Reminder box), and ensure that conditions for including a contextual identification have been met.
- Director, Corporate and Operational Policy (COP), or any other person designated to act in this position, is the Approval Authority for one-time CEO reports.
- [redacted] or any other person designated to act in this position, is the Approval Authority for one-time reports that will be shared with Second Parties.

Remember: OPS-1 report release sign-off responsibilities refer to categories of reports ("OPS-1a, 1b, 1c, or 1e") with a Canadian privacy angle that require [redacted] or DC SIGINT sign-off. Such reports are either based on private communications or communications of a Canadian outside Canada, or they contain information about Canadians. See CSOI-4-1, *SIGINT Reporting*, Appendix L, paragraph L4 for details on these categories.

5.6 Conditions for Obtaining a One-Time Approval

To apply for a one-time approval, all these conditions must be met:

1. contextual identification is the only available option
2. including the contextual identification increases the report's foreign intelligence value, and
3. distribution is limited as much as possible, for example, CEO or using a CSE AUSCANNZUKUS mask as opposed to a [redacted] mask.

5.7 Process for Obtaining a One-Time Approval

The following table illustrates the step-by-step process for obtaining one-time approvals.

Attention: Anyone in this chain may deny the request at any stage.

Step	Who Does It	Action
1	Analyst	ensures that • the appropriate OPS-1 box (a, b, c, or e) is ticked off, and • the contextual identification box is also ticked off in Section B (Special Content) of the Report Product Release Form
2	Reviewing Manager	• ensures that the conditions for contextual identification are met • signs the appropriate box • e-mails the request to Operational Policy • obtains [redacted] or DC SIGINT sign off • informs Operational Policy of the results
3	[redacted] (for OPS-1c) **or** DC SIGINT (for OPS-1a, b or e)	signs the appropriate place for • the relevant OPS-1 type, and • contextual identification approval
4	Operational Policy	• CEO reports – forwards e-mail to Director, COP • 5-eyes reports – forwards e-mail to [redacted], via Director, COP
5	Director, COP **or** [redacted]	approves and returns to Reviewing Manager via Operational Policy

Special circumstances: Where a Canadian faces or poses an imminent physical threat to safety (that is, an event that could jeopardize the life or well-being of any person, and which is to occur within 24 hours or less), or during silent hours, SIGINT Managers (that is, Program Managers or Program Line Managers) may approve a report on a one-time basis only. The designated authority must provide written approval *post factum*.

Requesting Approval – Blanket

5.8 Senior Management Approval

The following table sets out the authorities for blanket approvals:

If the report is...	Then blanket approval is...
CEO	[redacted]
shared with Second Parties	DC SIGINT[redacted]

Anyone officially designated to act in these positions may also approve these reports.

5.9 Process for Obtaining a Blanket Approval

To apply for a blanket approval, all these conditions must be met:

1. contextual identification is the only available option
2. including the contextual identification increases the report's foreign intelligence value, and
3. distribution is limited as much as possible, for example, CEO or using a CSE AUSCANNZUKUS mask as opposed to a [redacted] mask.

5.10 Process for Obtaining a Blanket Approval

The following table illustrates the step-by-step process for obtaining a blanket approval.

Attention: Anyone in this chain may deny the request at any stage.

Step	Who Does It	Action
1	Analyst	prepares the request for contextual identification
2	Reviewing Manager	ensures that the conditions for contextual identification are met
3	[redacted] (for CEO) **or** DC SIGINT (for reports shared with Second Parties)	• approves the request, and • forwards it to [redacted], if approved • informs the Reviewing Manager if denied

Continued on next page

5.10 Process for Obtaining a Blanket Approval (continued)

Step	Who Does It	Action
4	[redacted]	• approves the request, and • sends approval to Reviewing Manager via Operational Policy
5	Operational Policy	forwards the approval to SIGINT Operational Support for posting (cc SIGINT Programs Oversight and Compliance (SPOC))

5.11 Normal Sign-offs Still Required for Reports Issued Under Blanket Approval

Despite having obtained a blanket approval to contextually identify a Canadian on an ongoing basis, you must still ensure that all your reports are signed off by the normal chain of managers. For example, a series of reports that falls under the OPS-1c category but for which there is a blanket approval for contextual identification must still be signed by [redacted] for the OPS-1c aspect of the report.

5.12 Posting of Blanket Approvals

SIGINT Operational Support is responsible for posting blanket approvals on the Intelligence Branch's website, and for ensuring the list is kept up-to-date.

5.13 Time Limits and Renewals

You must remember that blanket approvals are given for specified periods of time, usually one calendar year:

- managers may request extensions for the blanket exemption, and
- [redacted] or DC SIGINT, [redacted] must reapprove each request for extension.

Contextual Identification of a Second Party Identity

5.14 Contextual Identification of Second Party Identities

Since CSEC is also responsible for protecting Second Party identities, if the contextual identity in question is Second Party, you must either:

- use a contextual identification that is certain to be acceptable to the Second Party, for example:
  - it has been used before in reporting
  - there is a Blanket Dissemination Authority (BDA) in place for the entity (NSA only), or
  - your team has received written confirmation from the Oversight or Compliance area at the Second Party that your wording is acceptable, or
- conduct a sensi-check with the relevant Liaison Office to find out what contextual reference phraseology the Second Party would prefer.

6. Threat-to-Life Reporting

6.1 What is Threat to Life Reporting?

Threat-to-life reporting is produced in support of time-sensitive operations of significant national security impact. Such situations may involve circumstances where a Canadian:

- is being held hostage by any foreign group (that is, kidnapped) or imprisoned by an unfriendly government
- is in a life-threatening situation, or
- may be involved in planning to commit, has committed, or may have been involved in the commission of acts that threaten the lives or safety of anyone regardless of nationality or location.

In such cases, Canadian identities must be available to relevant clients as quickly as possible to mitigate the above risks, or for foreign intelligence value. This is why, exceptionally and with senior management approval, you have two options:

1. name the Canadian in the report, or
2. suppress the identity and then provide it to specific recipients via separate channels (usually via e-mail) simultaneously with the wider release of reports where the identity is suppressed.

6.2 Conditions for Naming a Canadian

You may name Canadians in reports (or provide the identities to recipients via separate channels) under the following conditions:

1. it must be threat-to-life reporting as described in paragraph 6.1 (or other justifiable similar situations), and
2. the distribution must be limited as much as possible and must conform to conditions set out in each exemption approval, but may include Second Parties.

Requesting Approval – One Time

6.3 Senior Management Approval

You must obtain senior management approval to name or provide an advance release of Canadian identities in threat-to-life reporting.

- [redacted] or DC SIGINT, or any person designated to act in these positions, must assess the report as part of their OPS-1 report release sign-off responsibilities (see Reminder box in paragraph 5.5), and ensure that conditions for naming the person have been met.
- Director, COP, or any other person designated to act in this position, is the Approval Authority for one-time threat-to-life reporting.
- [redacted] or any other person designated to act in this position, is the Approval Authority for one-time reports that will be shared with Second Parties.

6.4 Process for Obtaining a One-Time Approval

The following table illustrates the step-by-step process for obtaining one-time approvals.

Attention: Anyone in this chain may deny the request at any stage.

Step	Who Does It	Action
1	Analyst	ensures that the appropriate OPS-1 box (a, b, c or e) is ticked off
2	Reviewing Manager	• ensures that: o the threat-to-life situation is real, and o the conditions in paragraph 6.2 are met • signs the appropriate box • e-mails the request (including the report) to Operational Policy, and • obtains [redacted] or DC SIGINT sign off

Continued on next page

6.4 Process for Obtaining a One-Time Approval (continued)

Step	Who Does It	Action
3	• [redacted] for (OPS-1c) **or** • DC SIGINT (for OPS-1a, b, or e)	signs in the appropriate place
4	Operational Policy	• CEO reports – forwards e-mail to Director, COP • 5-eyes reports – forwards e-mail to [redacted] via Director, COP
5	Director, COP or [redacted]	approves and returns to the Reviewing Manager via Operational Policy

Silent Hours: During silent hours, SIGINT Managers may approve a threat-to-life report on a one-time basis only. The designated authority must provide written approval *post factum*.

Requesting Approval - Blanket

6.5 Senior Management Approval

The following table lays out the authorities for blanket approvals:

If the report is ...	Then blanket approval is ...
CEO	[redacted] **and** [redacted]
shared with Second Parties	DC SIGINT [redacted]

Any other person officially designated to act in these positions may also act as Approval Authority.

6.6 Process for Obtaining Blanket Approval

The following table illustrates the step-by-step process for obtaining blanket approvals.

> **Attention:** Anyone in this chain may deny the request at any stage.

Step	Who Does It	Action
1	Analyst	prepares the request for naming in threat-to-life situations
2	Reviewing Manager	ensures that the criteria for threat-to-life naming are met
3	[redacted] (for CEO) **or** DC SIGINT (for reports shared with Second Parties)	• approves the request • signs and forwards it to [redacted] • informs the Reviewing Manager if denied
4	[redacted]	• approves the request • sends approval to Reviewing Manager via Operational Policy
5	Operational Policy	forwards the approval to SIGINT Operational Support (for posting) (c.c. SPOC)

6.7 Posting of Blanket Approvals

SIGINT Operational Support is responsible for posting blanket approvals on the Intelligence Branch's website and for ensuring that the list is kept up-to-date.

6.8 Time Limits and Renewals

You must remember that blanket approvals are given for specified periods of time, usually one calendar year:

- managers may request extensions for the blanket exemption, and
- [redacted] or DC SIGINT [redacted] must reapprove each request for extension.

6.9 Tracking Released Identities

Managers are responsible for giving Operational Policy the serial numbers of reports that were issued under threat-to-life blanket approvals. This is because Operational Policy must track all identities released, to:

- provide these statistics to the Minister of National Defence in the annual report
- provide these statistics to the Office of the CSE Commissioner (OCSEC), who regularly reviews releases of identities, and
- consider *post factum* disclosure risk management factors when identities are released to law enforcement agencies.

7. Naming Canadians [redacted]

7.1 The Rule

It is not unusual to find a Canadian, usually with dual citizenship, [redacted] for example, [redacted]

Although such a Canadian is considered to be [redacted] privacy protection measures still apply. This means that you may only use generic terms to refer to the person unless you apply to identify the Canadian by name and follow reporting conditions set out in paragraph 7.3.

7.2 Approval to Name a Canadian [redacted]

To name a Canadian [redacted] you must obtain [redacted] authorization via your Supervisor. The Supervisor must advise the Manager, Operational Policy and SPOC when the request has been approved. Operational Policy will in turn advise its counterparts at Second Party agencies. Operational Policy will alert SIGINT Operational Support, who will post the authorized naming on the Intelligence Branch's website.

If Second Parties identify a Canadian [redacted] and wish to name the person in reporting, they must request permission from Operational Policy, who will consult [redacted]

Attention: You must not name Canadians [redacted] You may name Canadians in international organizations such as the UN only by title, if necessary.

7.3 Reporting Conditions

The report in which you name the Canadian [redacted] must meet the following conditions:

- you must not indicate that he or she has any kind of Canadian status (that is, citizenship or permanent residency)
- you must focus exclusively on the Canadian's [redacted]
- if and when this Canadian person [redacted], you must stop naming him or her, and must not footnote reports that did name this person [redacted] This will ensure that the person cannot be directly or contextually identified through earlier reporting, and
- if the person [redacted] you may continue to name this person as long as he or she [redacted] This table lays out the circumstances.

Attention: You do not have to obtain OPS-1c approval sign offs for reports that name a Canadian [redacted] unless it includes information about another Canadian.

If a Canadian...	and...	then...
[redacted]	[redacted]	• you must no longer name that person, and • in future reports, you may not refer to those earlier reports in which that person had been named
		you may continue to name that person until such time as the person [redacted]

7.4 Posting of Approvals

SIGINT Operational Support is responsible for posting [redacted] authorizations in force to name Canadians [redacted] on the Intelligence Branch's website.

8. Inadvertent Naming and Retroactive Approval

8.1 The Rule

You must notify Operational Policy when you inadvertently name a Canadian or Second Party person, corporation or organization in a report. Generally speaking, when this happens, you will be asked to cancel and reissue the report with the identity suppressed. However, in exceptional circumstances (for example, when you have inadvertently named a person in a large number of reports over a long period of time), you may be able to apply for retroactive approval (see paragraphs 8.3 through 8.6).

8.2 Actions Taken by Operational Policy

Canadians inadvertently named:

- in CSEC reports, Operational Policy will ensure that the relevant CSEC reporting element cancels and reissues the report with the identity suppressed, and
- in Second Party reports, Operational Policy will ask the relevant Second Party to cancel and reissue the report, with the Canadian identities suppressed.

In both instances, Operational Policy will enter the details and the corrective measures taken into the Privacy Incidents File.

Second Parties inadvertently named in CSEC reports:

Operational Policy will ensure that the relevant CSEC reporting element cancels and reissues the report with the identity suppressed.

Retroactive Approval

8.3 The Rule

Generally speaking, you must cancel and reissue reports in which you inadvertently named or contextually identified Canadians or Second Parties. However, after issuing a number of reports (more than 10) in which you named or contextually identified Canadians or Second Parties you believed to be foreign, you may learn that the person, corporation or organization is actually Canadian (or Second Party). In this case, you *may* be able to obtain retroactive blanket approval for these historical reports.

8.4 Retroactive Blanket Approval – Canadian Identity

You must contact Operational Policy, who will assess retroactive blanket approval requests on a case-by-case basis. The Director, COP is responsible for granting retroactive blanket approvals.

With a retroactive blanket approval you do not need to cancel or reissue these 10 or more historical reports since this might draw unwanted attention to the inadvertently identified Canadian.

8.5 Retroactive Blanket Approval – Second Party Identity

If the identity you have named or contextually identified in the series of reports is from a Second Party country, you must immediately notify Operational Policy, who will ask the relevant Second Party how they want to handle the situation.

You should not assume that retroactive approval will be forthcoming from that Second Party. Decisions made by the Second Party are final.

8.6 Handling of Identities in Future Reports

Retroactive approval received for previously issued reports does not extend to future reporting. If you obtained retroactive approval, and then you have further need to name the Canadian or Second Party, contextually or otherwise, you must follow these procedures to obtain the required approvals.

Furthermore, in order to limit the damage caused by identifying the person, corporation or organization, you must not mention in reports, or use footnotes to point to earlier reporting where the identity was not suppressed, even if the earlier reports did not focus on the identified Canadian or Second Party.

9. Responsibilities for Applying Naming Rules

9.1 Roles and Responsibilities

The following table outlines the key roles and responsibilities in applying the rules for suppressing or naming Canadians or Second Party people, organizations or corporations.

Who	Responsibility
DC SIGINT	Granting blanket approval for contextual identification and threat-to-life naming of reports to be released to Second Parties, with DGPC
DGPC	• Approving one-time contextual identification and threat-to-life naming in reports to be released to Second Parties • Granting blanket approval for contextual identification and threat-to-life naming in reports to be released to Second Parties, with DC SIGINT
[redacted]	• Granting blanket approval for contextual identification and threat-to-life naming in CEO reports • Authorizing naming of Canadians [redacted]
Director, COP	• Approving one-time contextual and threat-to-life identifications in CEO reporting • Authorizing requests for retroactive blanket approvals in cases of inadvertent naming
[redacted] Managers	• Ensuring that o conditions for contextual identifications are met (one-time and blanket), and o threat-to-life situations are real • Forwarding to Operational Policy: o one-time contextual identification requests o one-time threat-to-life naming requests to Operational Policy • Approving threat-to-life reporting on a one-time basis only during silent hours
[redacted] Supervisors	• Obtaining [redacted] authorization to name a Canadian [redacted] • Advising Manager, Operational Policy, and SPOC that the request has been approved

Continued on next page

Who	Responsibility
Operational Policy	• Clarifying the status of Canadian or Second Party persons • Releasing suppressed Canadian or Second Party identities • Advising Second Party agencies of authorizations to name Canadians [redacted] • Taking appropriate action when Canadian identities are inadvertently named in CSEC or Second Party reports • Assessing requests for retroactive approval and forwarding to Director, COP for authorization • Forwarding blanket approvals to identify Canadians by name or contextually to SIGINT Operational Support
[redacted]	• Posting blanket approvals for contextual identifications and threat-to-life naming, and [redacted] authorizations to name Canadians [redacted] on the Intelligence Branch website • Ensuring the lists are up-to-date
Reporting elements	• Cancelling and reissuing reports with Canadian and/or Second Party identities appropriately suppressed • Sending requests for ○ one-time naming and blanket approvals to [redacted] and [redacted] or [redacted] ○ naming of Canadians [redacted] to [redacted] and ○ retroactive approvals to [redacted] as set out in these procedures

10. Information About These Procedures

10.1 Accountability

The following table outlines accountability for revising, reviewing, recommending and approving these procedures.

Who	What
DC SIGINT	Approves these procedures
DGPC	Recommends these procedures
General Counsel, DLS	• Reviews these procedures to ensure they comply with the law • Provides legal advice, when requested
Operational Policy	Revises these procedures as required

10.2 References

- *National Defence Act*
- *Privacy Act*
- *Ministerial Directive on the Privacy of Canadians*, June 2001
- *Ministerial Directive on CSE's Accountability Framework,* June 2001
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC's Activities*
- OPS-1-1, *Procedures for Release of Suppressed Information from SIGINT Reports*
- OPS-2-3, *Sensi-Check Procedures*
- OPS-5-3, *Write-to-Release (WTR) Procedures*
- CSOI-4-1, *SIGINT Reporting*
- *Canadian SIGINT Report Review/Release Authorities*
- IRRELEVANT

10.3 Enquiries

Direct any questions about these procedures to CSEC Supervisors and Managers, who in turn, will contact Operational Policy staff (e-mail [redacted] as necessary.

10.4 Amendments

Situations may arise where amendments to these procedures are required because of changing or unforeseen circumstances. Such amendments will be communicated to staff and will be posted on the Operational Policy website.

11. Definitions

11.1 Canadian

"Canadian" refers to
a) a Canadian citizen
b) a person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act* and who has not subsequently lost that status under that *Act*, or
c) a corporation incorporated under an Act of Parliament or of the legislature of a province.

(NDA, section 273.61)

For the purposes of these procedures, "Canadian organizations" are also accorded the same protection as Canadian citizens and corporations.

A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada.

11.2 Collateral

Information that is not derived from SIGINT. It is published in written form or broadcast in either audio or video form by a person or organization outside the SIGINT community. Collateral may be classified or unclassified.

11.3 Contextual Identification

A contextual identification is any description of a Canadian or Second Party person, corporation or organization that provides enough information for a reasonably informed person (that is, someone who routinely reads a major newspaper, watches TV news, or visits news websites) to be able to guess or research the actual identity.

11.4 [redacted] Identifiers

[redacted] identifiers [redacted] (for example, e-mails, IP addresses, [redacted]

11.5 Foreign

In the context of the NDA, and the *CSIS Act*, "foreign" refers to non-Canadians.

For the purpose of these procedures, foreign does not include Australian, New Zealand, UK or US people, corporations or organizations.

11.6 Foreign Intelligence

Foreign intelligence is information or intelligence relating to the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security. (NDA, section 273.61)

11.7 Government of Canada

In these procedures, a reference to the GC includes:

(a) the Senate
(b) the House of Commons
(c) the Library of Parliament
(d) any federal court
(e) any board commission or council, or other body or office, established to perform a governmental function by or pursuant to an Act of Parliament or by or under the authority of the Governor in Council
(f) a department or any portion of the GC
(g) a Crown Corporation established by or pursuant to an Act of Parliament, and
(h) any other body that is specified by an Act of Parliament to be an agent of Her Majesty in right of Canada or to be subject to the direction of the Governor in Council or a minister of the Crown.

This does not include

(i) any institution of the Council or government of the Northwest Territories or the Yukon Territory or of the Legislative Assembly or government of Nunavut, or
(j) any Indian band, band council or other body established to perform a governmental function in relation to an Indian band or other group of aboriginal people.

11.8 Identity

An identity is information that can be uniquely associated, directly or indirectly, with a Canadian or Second Party person, corporation or organization. It can include, for example, a name, [redacted] telephone number, e-mail address, IP address, passport number, [redacted]

11.9 Integree

An integree is a person seconded to CSEC from one of CSEC's cryptologic partner organizations.

11.10 Personal Information

Personal information is defined in the *Privacy Act* as "information about an identifiable individual that is recorded in any form". See Annex 1 for the complete definition.

11.11 Privacy Incidents File (PIF)

The PIF is a central record of privacy incidents to track and demonstrate CSEC's commitment to protect privacy, improve our own practices, ensure transparency, and enhance public confidence in CSEC. The reporting and tracking of privacy incidents is one of the measures in place to ensure legal compliance and enhances the overall privacy protection framework.

11.12 Report Actor

In CSEC's report database, the term "report actor" refers to anyone involved in the SIGINT reporting chain, from report author through to release authority.

11.13 Second Parties

Second Parties refer to CSEC's SIGINT counterparts:

- the US National Security Agency (NSA)
- the UK Government Communications Headquarters (GCHQ)
- Australia's Defence Signals Directorate (DSD), and
- New Zealand's Government Communications Security Bureau (GCSB).

11.14 Secondee

A secondee is an individual who is temporarily moved from another GC or private organization to CSEC, and who at the end of the assignment returns to the originating organization.

11.15 Sensi-check

Sensi-checking is the process of:

- identifying nationally sensitive information in end-product reports
- ensuring that the nationally sensitive information is disseminated on a strict need-to-know basis without compromising the accuracy and usefulness of the intelligence overall.

11.16 Signals Intelligence (SIGINT)

SIGINT is the term given to information gathered about foreign countries by collecting and studying their radio, wire, radar and other electronic or electromagnetic transmissions. SIGINT comprises Communications Intelligence (COMINT), Electronic Intelligence (ELINT) and Foreign Instrumentation Signals Intelligence (FISINT).

11.17 SIGINT Reports

A SIGINT report refers to any report that is based on SIGINT. It includes, but is not limited to:

- End-product (a.k.a. SIGINT end-product, end-product reports): SIGINT reports that are issued in response to a GC Requirement (GCR). End-product conforms to established reporting standards (CSOI-4-1, *SIGINT Reporting*).
- Technical SIGINT reports, such as Cryptologic/Communications Information Reports (CIRs) [redacted] Technical SIGINT reports are usually issued solely to SIGINT producers, and are intended to aid in the further collection of SIGINT.
- Gists, consisting of raw and often unassessed SIGINT. They relate to indications and warnings (I&W) in connection with certain SIGINT targets; they are serialized and released using CSEC's report-writing tool
- Advance reports, which are informal, partially vetted SIGINT reports containing information that requires more analysis. They are intended as a vehicle for timely reporting of highly perishable intelligence.

[redacted]

11.18 Suppressed Information

Suppressed information is defined as information excluded from a SIGINT report because it may reveal the identity of a Canadian or Second Party person, corporation or organization. Suppressed identities are stored in a limited-access database or system and are replaced in the report by a generic term.

Continued on next page

11.18 Suppressed Information (continued)

Identities include but are not limited to, personal identifiers such as names, passport information, [redacted], e-mail addresses, phone numbers and IP addresses, [redacted]

11.19 Write-to-Release (WTR)

WTR is an initiative under which COMINT reports are issued at the lowest classification possible. WTR involves sanitizing, usually to the SECRET level, all key information that can be released outside COMINT channels. The result of this process is a report which contains COMINT and non-COMINT paragraphs.

Annex 1 – Personal Information

Definition of Personal Information in the *Privacy Act*

"Personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of sections 7, 8 and 26 and section 19 of the *Access to Information Act*, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,
  (i) the fact that the individual is or was an officer or employee of the government institution,
  (ii) the title, business address and telephone number of the individual,
  (iii) the classification, salary range and responsibilities of the position held by the individual,
  (iv) the name of the individual on a document prepared by the individual in the course of employment, and
  (v) the personal opinions of views of the individual given in the course of employment,

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years.

Annex 2 – Canadian Naming Examples

A2.1 Canadians in Canada

A2.1.1 Persons in Canada

These are some examples of people in Canada who may appear in traffic:

Entity in Traffic	Suggested wording in report
Named Canadian **citizen**	"a Canadian citizen"
Honorary Canadian citizen	use name in report
Named **permanent resident** of Canada	"a Canadian resident"
Named **deceased Canadian** citizen or permanent resident (dead **less** than 20 years)	"a deceased Canadian"
Named **deceased Canadian** citizen or permanent resident (dead **more** than 20 years)	use name in report
Named **foreigner in Canada**, including those on special visas (for example, student or work visa)	use name in report
Honorary Consul in Canada	"a named Canadian"
[redacted]	use name in report
	use name in report (once status has been granted, you must suppress the name)
Named **Second Party national** in Canada	use generic term, for example, "an Australian person"
[redacted]	"a Canadian citizen"
Named **Canadian member of an identified** terrorist group in Canada	"a Canadian member of the [redacted]

A2.2 Canadians outside Canada

A2.2.1 Canadians Outside Canada

These are a few examples of Canadians in roles outside Canada:

Entity in Traffic	Suggested wording in report
[redacted]	With the authorization of [redacted] use name in report with no reference to Canadian status
Canadian working for a terrorist group	use generic identity (for example, "a named Canadian known to be a member of [redacted])
Canadian working for a named international organization	use title if necessary for clarity, with no reference to Canadian status

A2.3 GC Officials

A2.3.1 GC Officials

These are examples of GC officials:

Entity in Traffic	Suggested wording in report
Canadian Member of Parliament or Senator acting in an official capacity	use generic wording such as "a Canadian Member of Parliament"
Speaker of the House	use generic wording "a Canadian Member of Parliament"
Current Cabinet Ministers acting in their official capacity	use title if necessary for clarity, for example, "Minister of National Defence", otherwise use generic term "a senior Canadian official"
Name of an opposition party	"an opposition party"
Name of "the Official Opposition"	avoid reference in report, use "an opposition party"
Name of the governing party	"the governing party"

Continued on next page

A2.3.1 GC Officials (continued)

Entity in Traffic	Suggested wording in report
Senior Federal Public Servants	use title only if necessary for clarity, for example, "Director General, [redacted], otherwise use a generic term "a [redacted] official"
[redacted]	
General in Canadian Forces	use title if necessary for clarity, for example, "Canadian General stationed in [redacted], otherwise use generic term, "a senior Canadian military official"

A2.4 Provincial, Territorial and Municipal People, Corporations and Organizations

A2.4.1 Provincial, Territorial and Municipal

These are examples of people, corporations and organizations in provincial, territorial and municipal governments:

Entity in Traffic	Suggested wording in report
The Premier of Ontario	In CEO reports, use "the premier of a Canadian province". In other reports, use "a senior provincial official"
Toronto	use name when it serves as a geographic reference; otherwise use "a Canadian city"

A2.5 Non-Governmental Organizations

A2.5.1 Non-Governmental Organizations

These are examples of non-governmental organizations and corporations in Canada:

Entity in Text[redacted]	Suggested wording in report
The President of [redacted] Inc.	"a senior official of a Canadian company"
[redacted] Inc. (incorporated in Canada)	"a Canadian company"
[redacted] Inc.'s parent company, incorporated in [redacted])	use in report
Canadian president of [redacted] Canada Ltd., a subsidiary of [redacted]-based [redacted]	"senior official of a Canadian subsidiary of a [redacted] firm"
[redacted] Ltd. of [redacted]	use in report
[redacted] (not incorporated in Canada)	use in report
[redacted] (used as a brand name)	use in report, for example, [redacted]
[redacted]	
[redacted] located in Toronto	use in report
[redacted]	
Festivals, exhibitions or conferences	use in report, provided the activities or its organizers are not discussed

A2.6 [redacted] Identifiers

A2.6.1 [redacted]
Identifiers

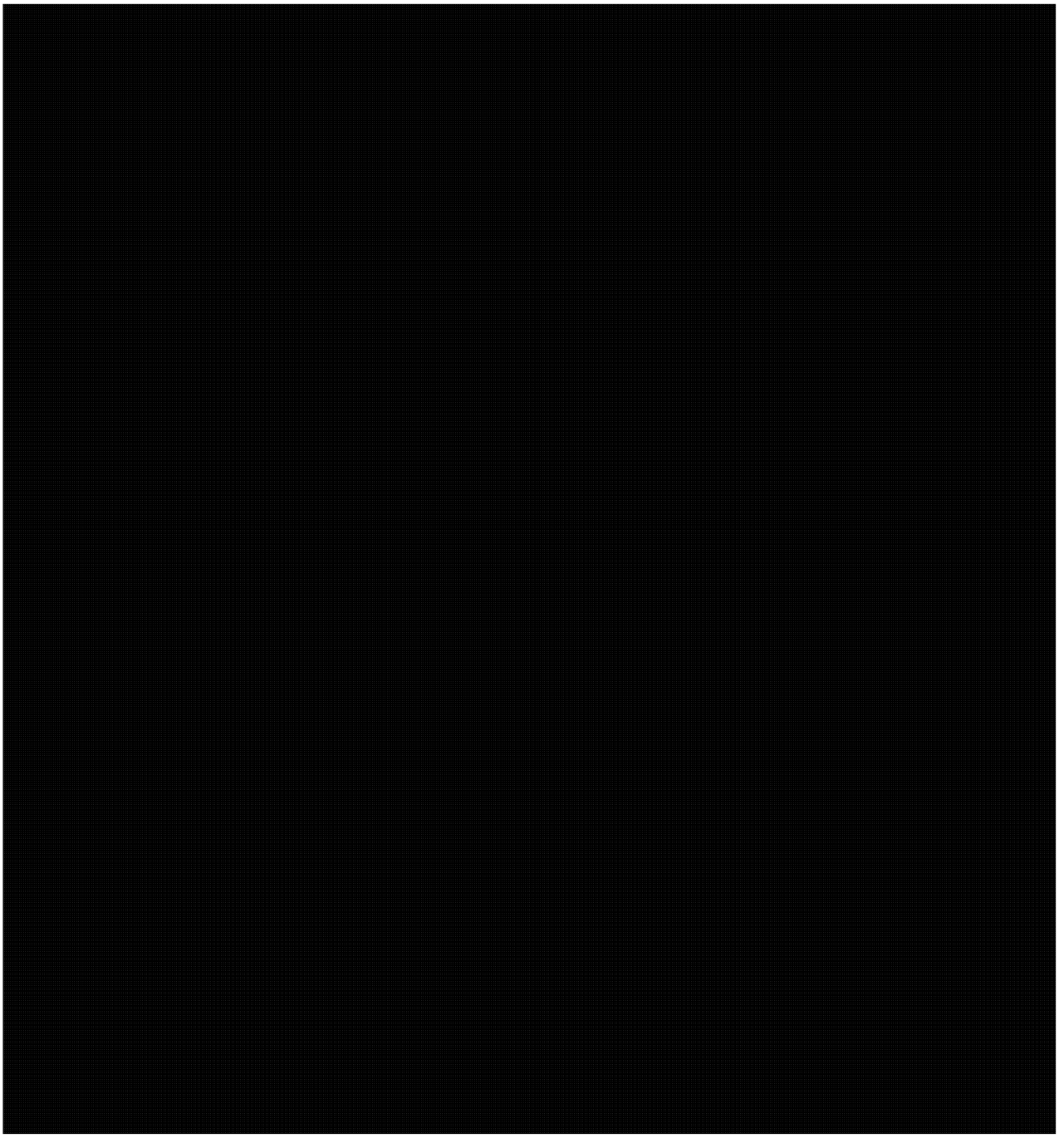
These are examples of different [redacted] identifiers:

[redacted]

A2.7 [redacted]

[redacted]

Annex 3 [redacted]



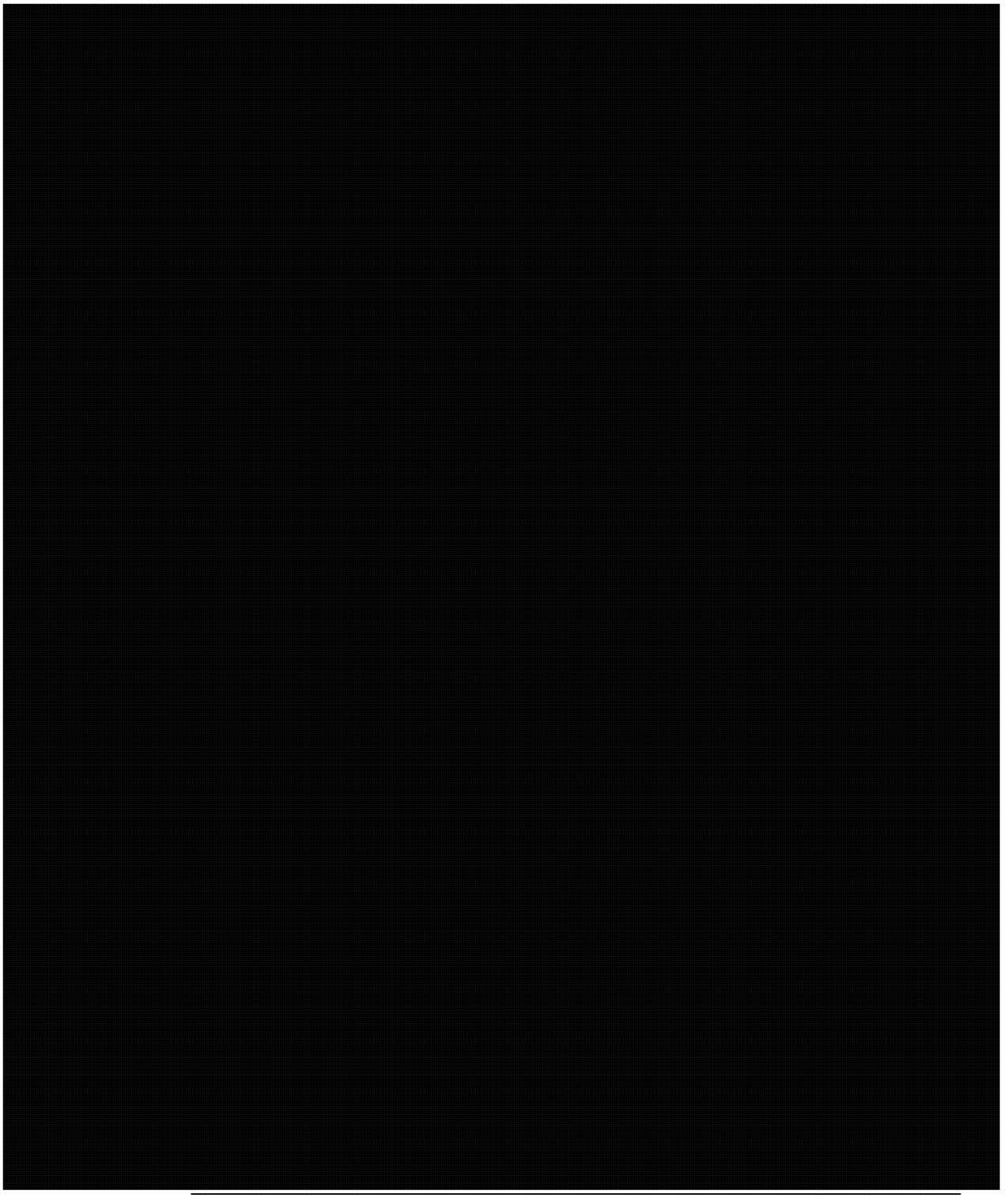
[redacted]

Continued on next page

Continued on next page

Annex 4 [redacted]

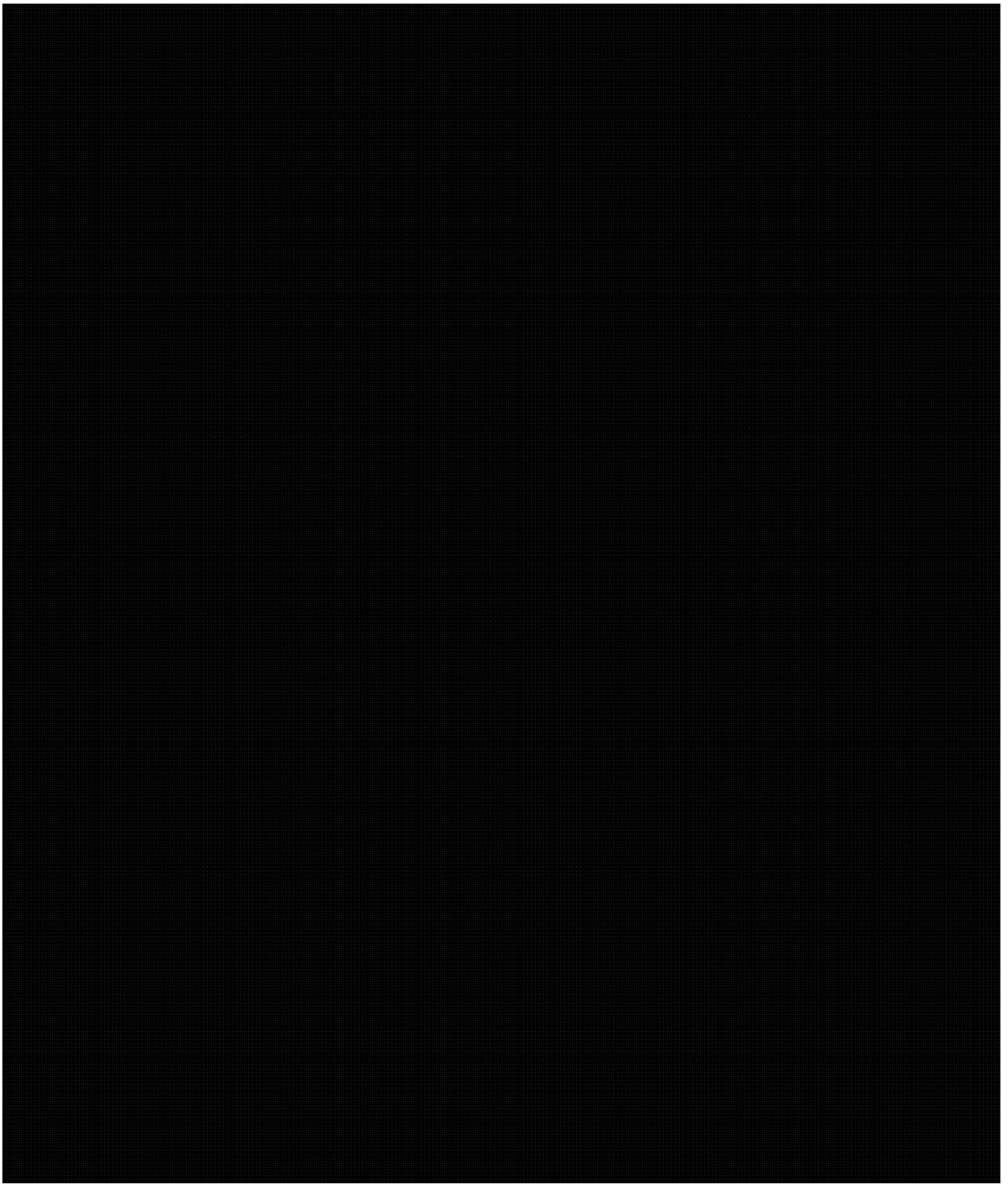
[redacted]



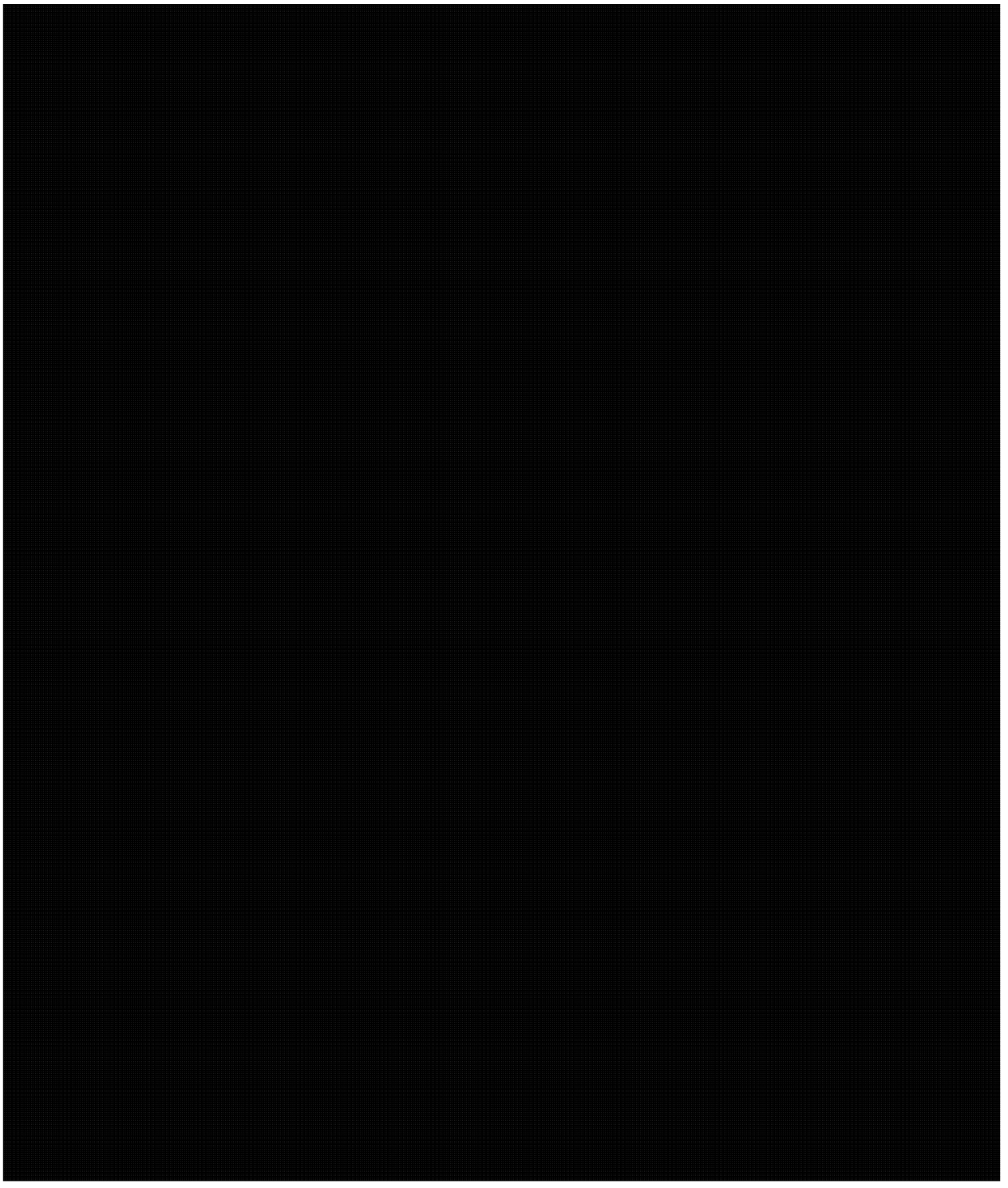
Annex 5 [redacted]

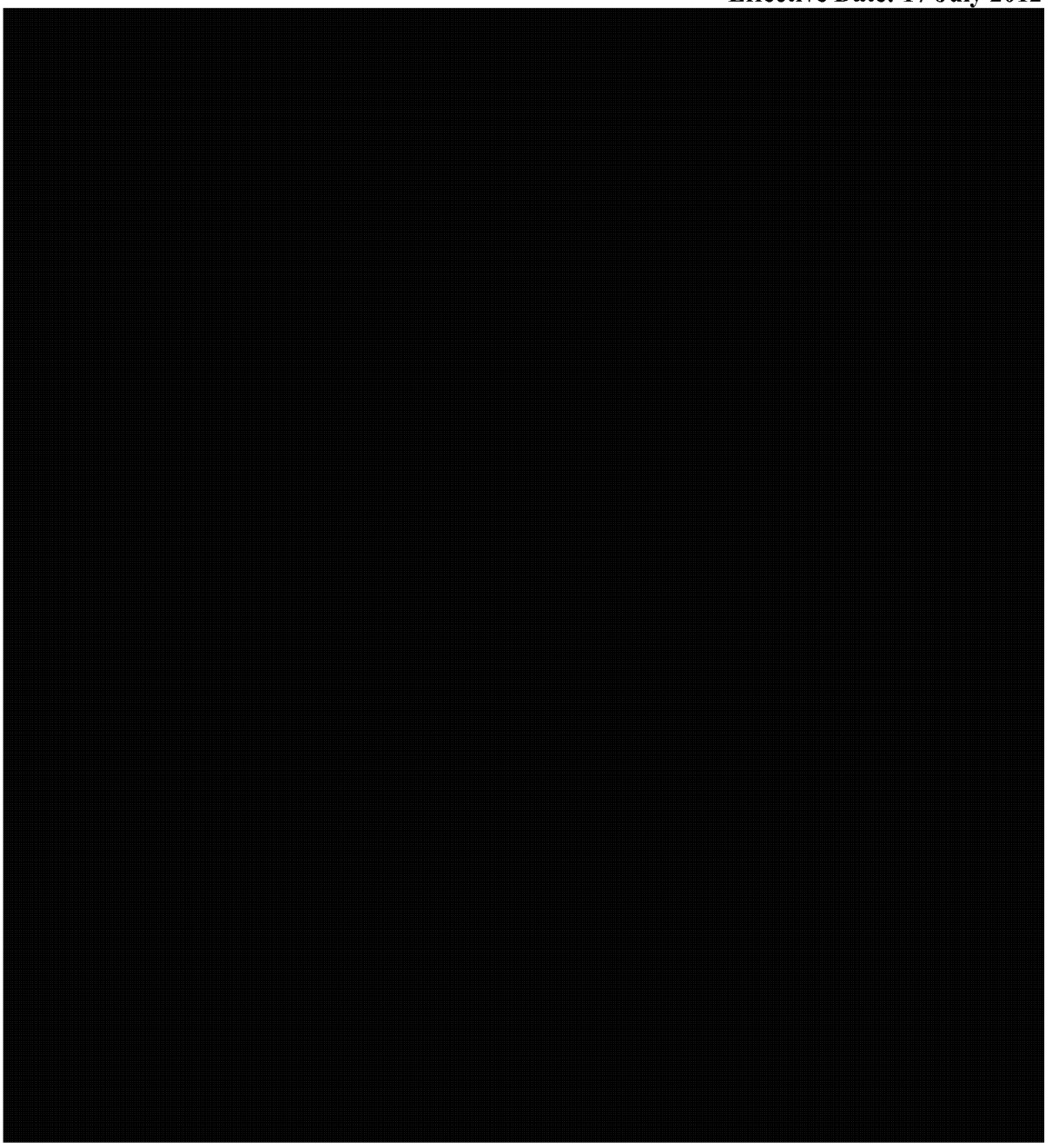
[redacted]

Continued on next page

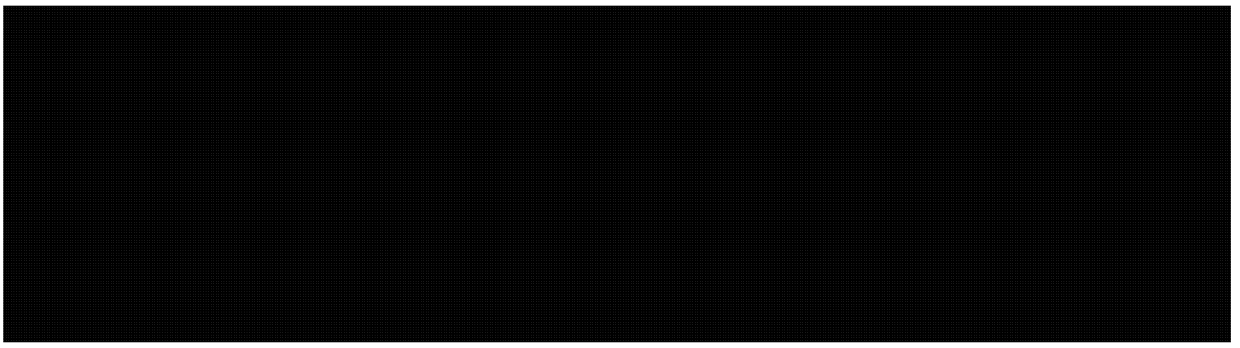


Continued on next page



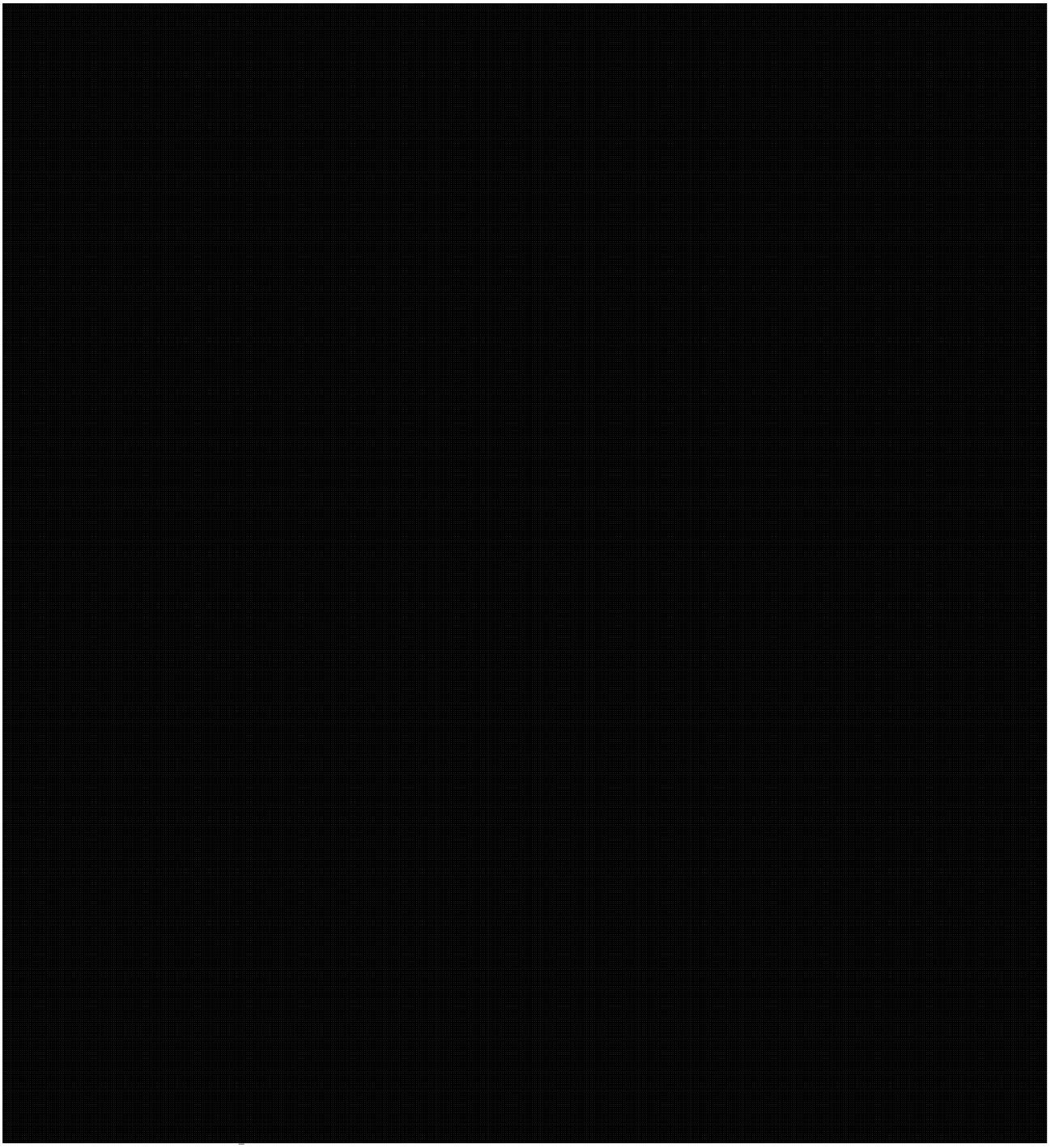


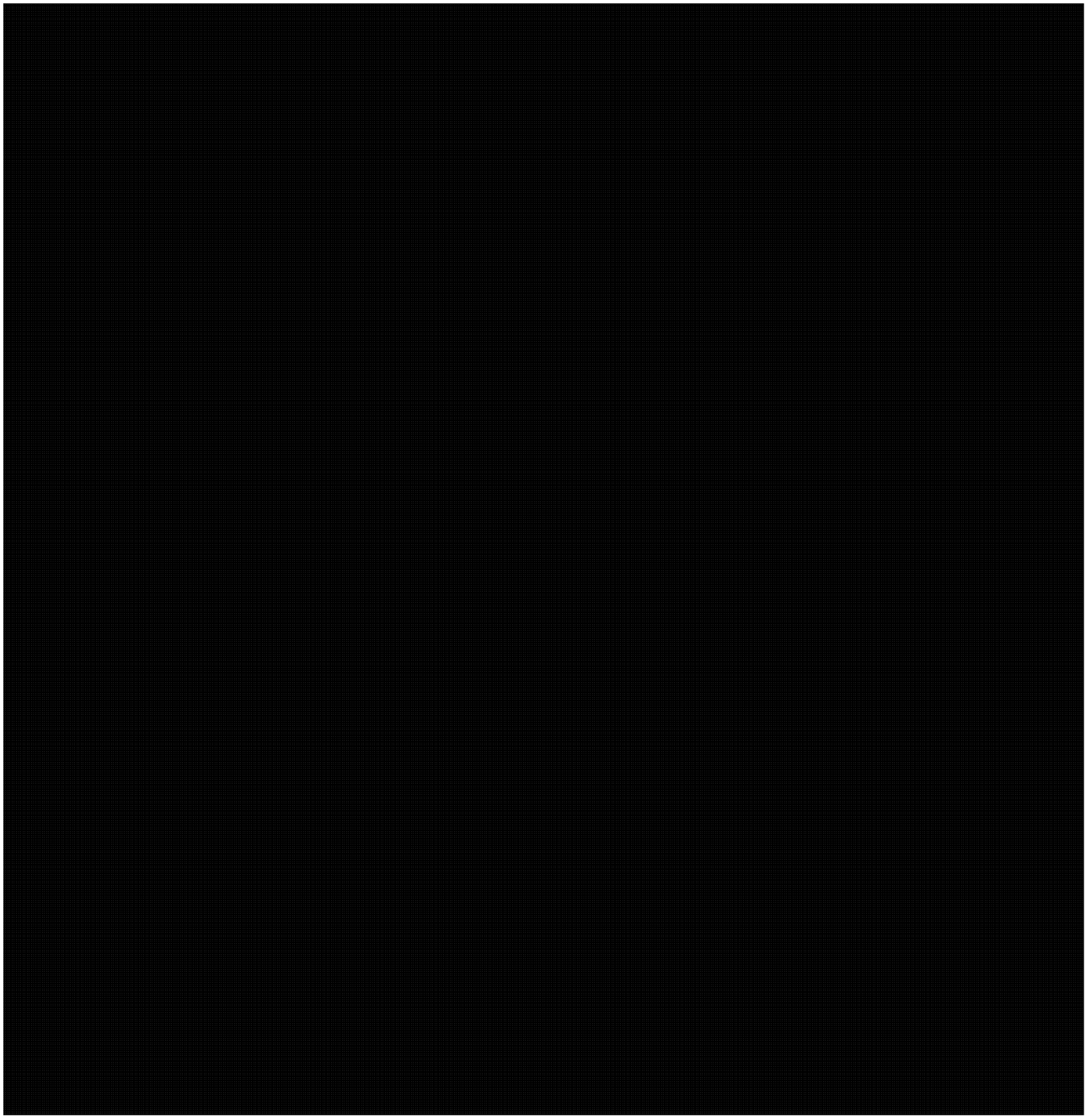
Continued on next page



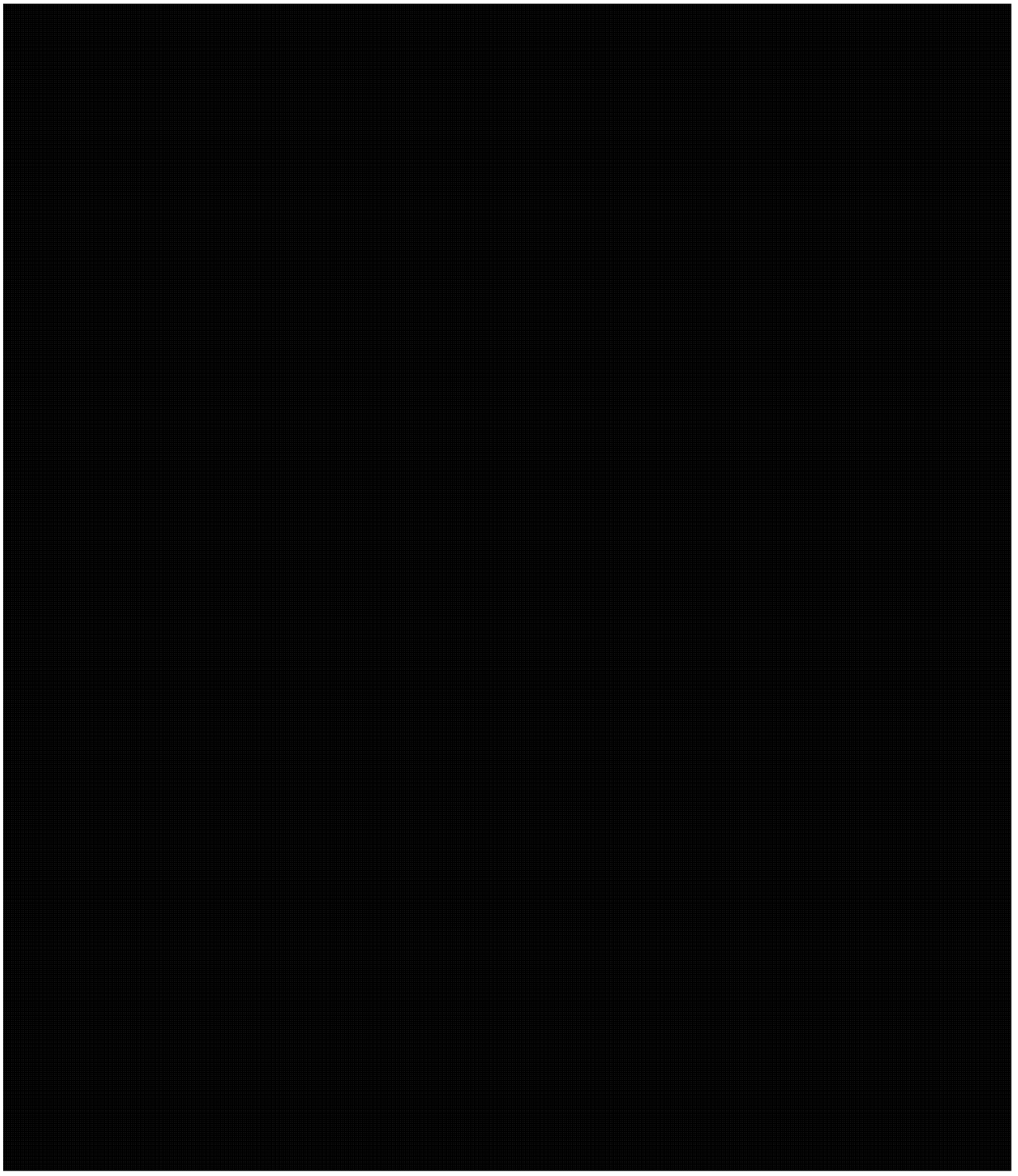
Annex 6 [redacted]

[redacted]

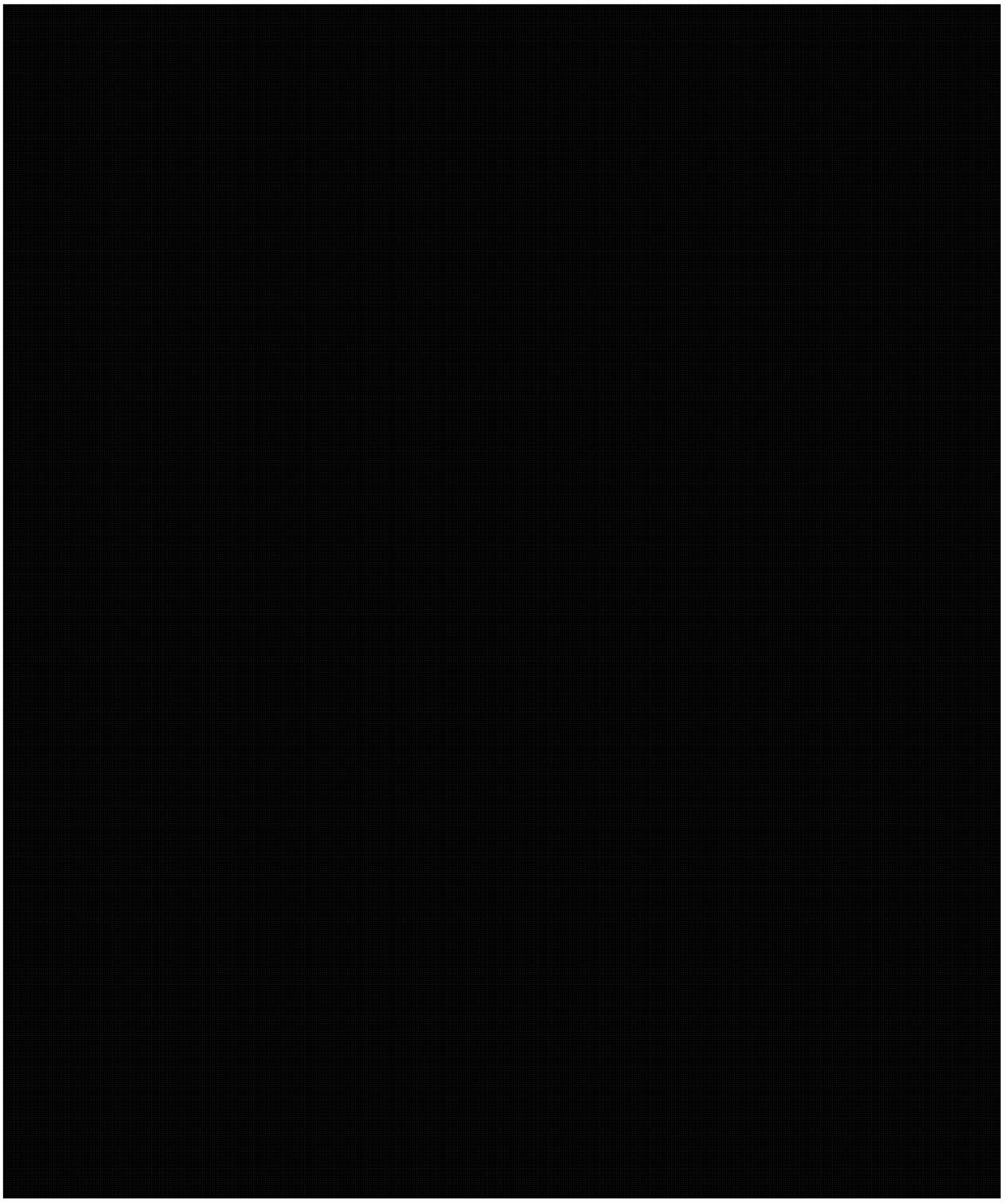




Continued on next page



Continued on next page



Continued on next page