Court File No. T-1492-17

FEDERAL COURT

BETWEEN:

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

Applicant

- and -

ATTORNEY GENERAL OF CANADA

Respondent

CERTIFIED TRIBUNAL RECORD

Volume XV

Minister of Public Safety | Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

OCT 26 2011

BY HAND **TOP SECRET // CEO**

Mr. Richard Fadden
Director
Canadian Security Intelligence Service
1941 Ogilvie Road
Gloucester, Ontario K1J 1B7

Dear Mr. Fadden:

Attached you will find my written Direction as per section 6(2) of the *Canadian Security Intelligence Service Act* with respect to intelligence priorities of the Service. This Ministerial Direction will replace the previous Ministerial Direction on Intelligence Priorities set out in 2010.

The new Ministerial Direction provides high-level guidance regarding intelligence priorities that were approved by the Cabinet Committee on National Security on July 28, 2011.

A copy of this letter and the enclosed Ministerial Direction will be sent to the Chair of the Security Intelligence Review Committee, and to the Inspector General of the Canadian Security Intelligence Service.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

Enclosure: (1)

CSIS / SCRS
OCT 27 [redacted]
[redacted]
DIR

Canada

MINISTERIAL DIRECTION TO THE DIRECTOR OF THE CANADIAN SECURITY INTELLIGENCE SERVICE: INTELLIGENCE PRIORITIES FOR 2011-2012

In July 2011, the Cabinet Committee on National Security approved the following Government of Canada Intelligence Priorities for 2011-2012 in order of importance: [redacted] These priorities direct Canadian intelligence collection, and inform the assessment and analysis of intelligence to ensure that it is aligned with broader government objectives.

Given this broad direction, this Ministerial Direction provides guidance to the Director of the Canadian Security Intelligence Service (CSIS), pursuant to subsection 6(2) of the *CSIS Act*, on the intelligence priorities 2011-2012 that reflects CSIS's mandate and capabilities. This guidance will also inform the development of CSIS specific intelligence requirements.

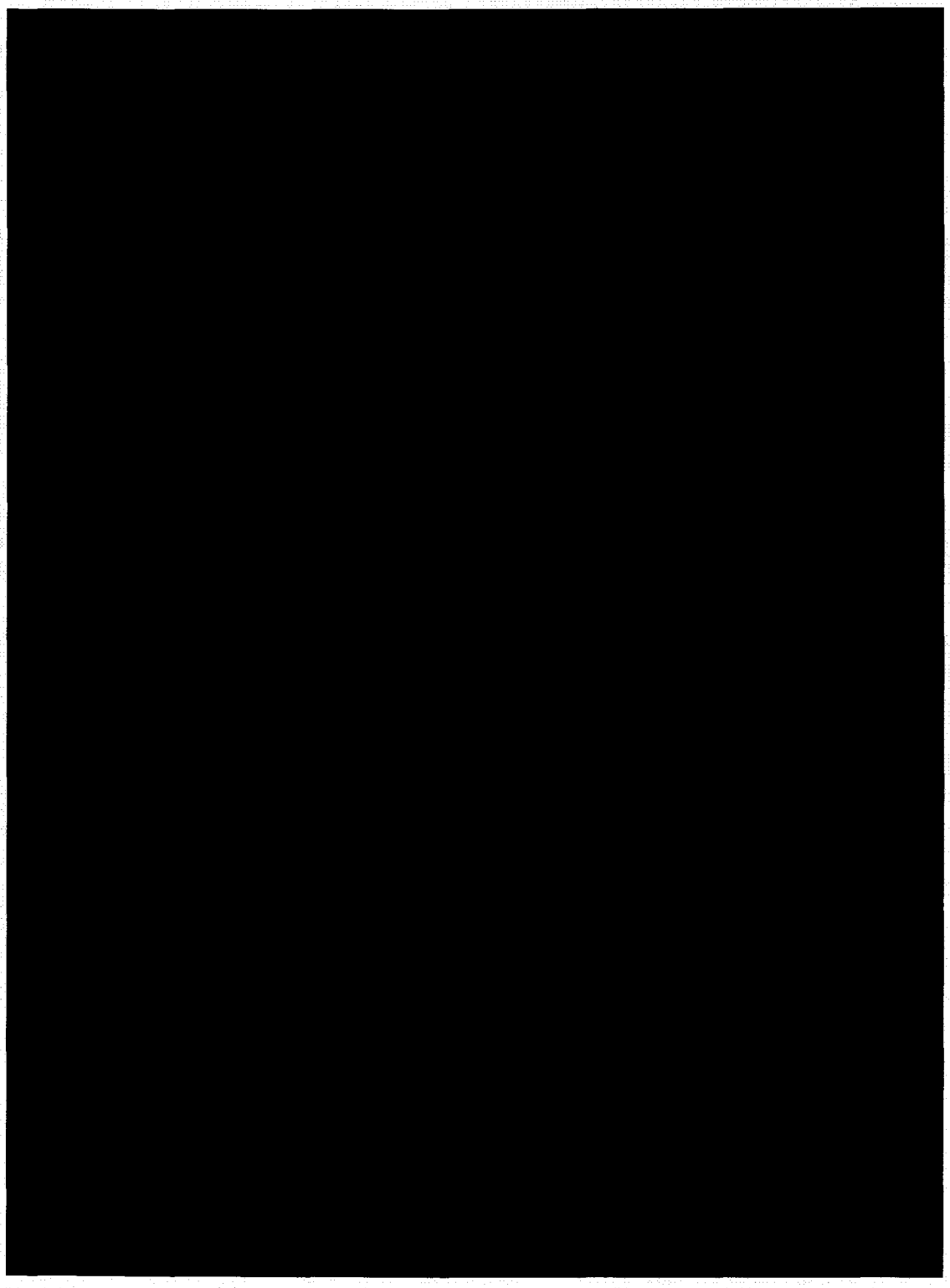
These intelligence priorities shall remain in effect until renewed or replaced by the Minister.

INTELLIGENCE PRIORITIES

Today's complex threat environment is increasingly global and fluid in nature, and intelligence continues to be the key to counter threats to the security of Canada posed by states, terrorist groups, foreign intelligence agencies, and other individuals and entities.

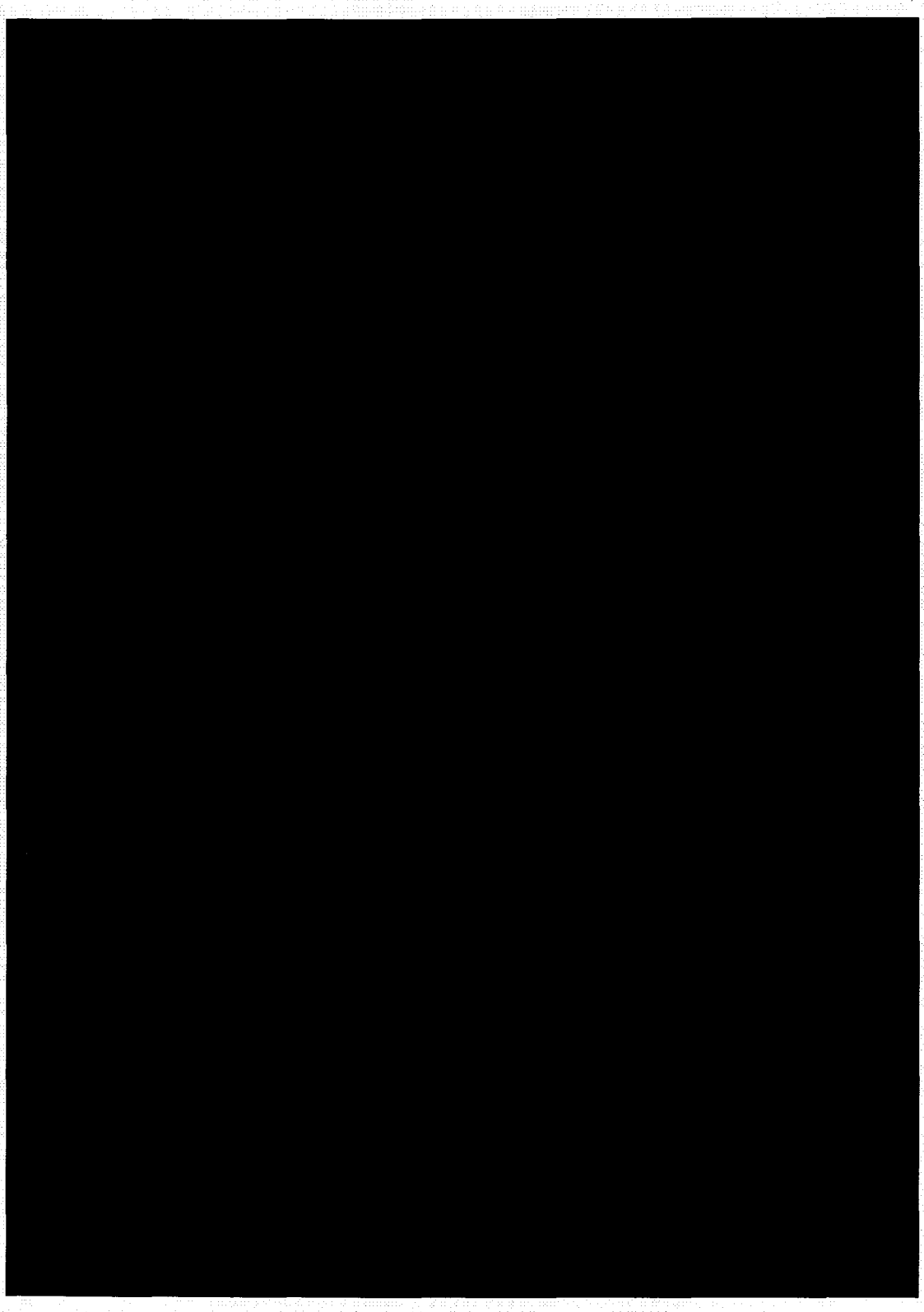
CSIS is directed to continue to collect information and intelligence both within Canada and abroad on threats to the security of Canada. Consistent with the priorities outlined herein, CSIS is directed to meet evolving intelligence needs and respond to emerging issues in a timely manner [redacted]

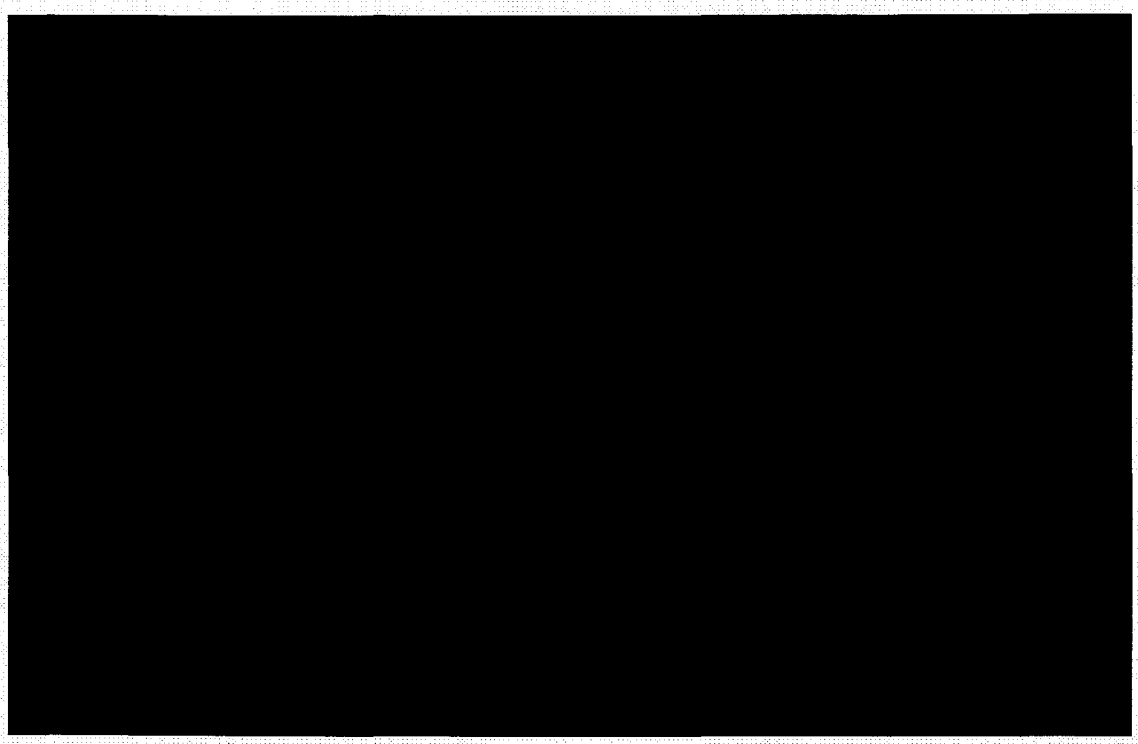
[redacted]



[redacted]

3/5





REPORTING TO THE MINISTER

Notwithstanding that CSIS advises the Government on an ongoing basis on threats to the security of Canada, the Director should report to the Minister of Public Safety, in a timely manner, on any significant risk to the security of Canada or potential for public controversy related to the Service's mandate.

In support of the National Security Expenditure report initiative, CSIS should work collaboratively with Public Safety officials to develop an effective means to account for how 2011-12 resource allocations relate to the new intelligence priorities with a view of including this assessment in the Director's annual report.

INSTRUCTIONS DU MINISTRE AU DIRECTEUR DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ : PRIORITÉS EN MATIÈRE DE RENSEIGNEMENT POUR 2011-2012

En juillet 2011, le Comité du Cabinet sur la sécurité nationale a approuvé les priorités suivantes du gouvernement du Canada en matière de renseignement pour 2011-2012 (en ordre d'importance) : t [redacted] Ces priorités orientent les activités de collecte de renseignements du Canada ainsi que l'évaluation et l'analyse des renseignements pour s'assurer qu'elles cadrent avec les grands objectifs du gouvernement.

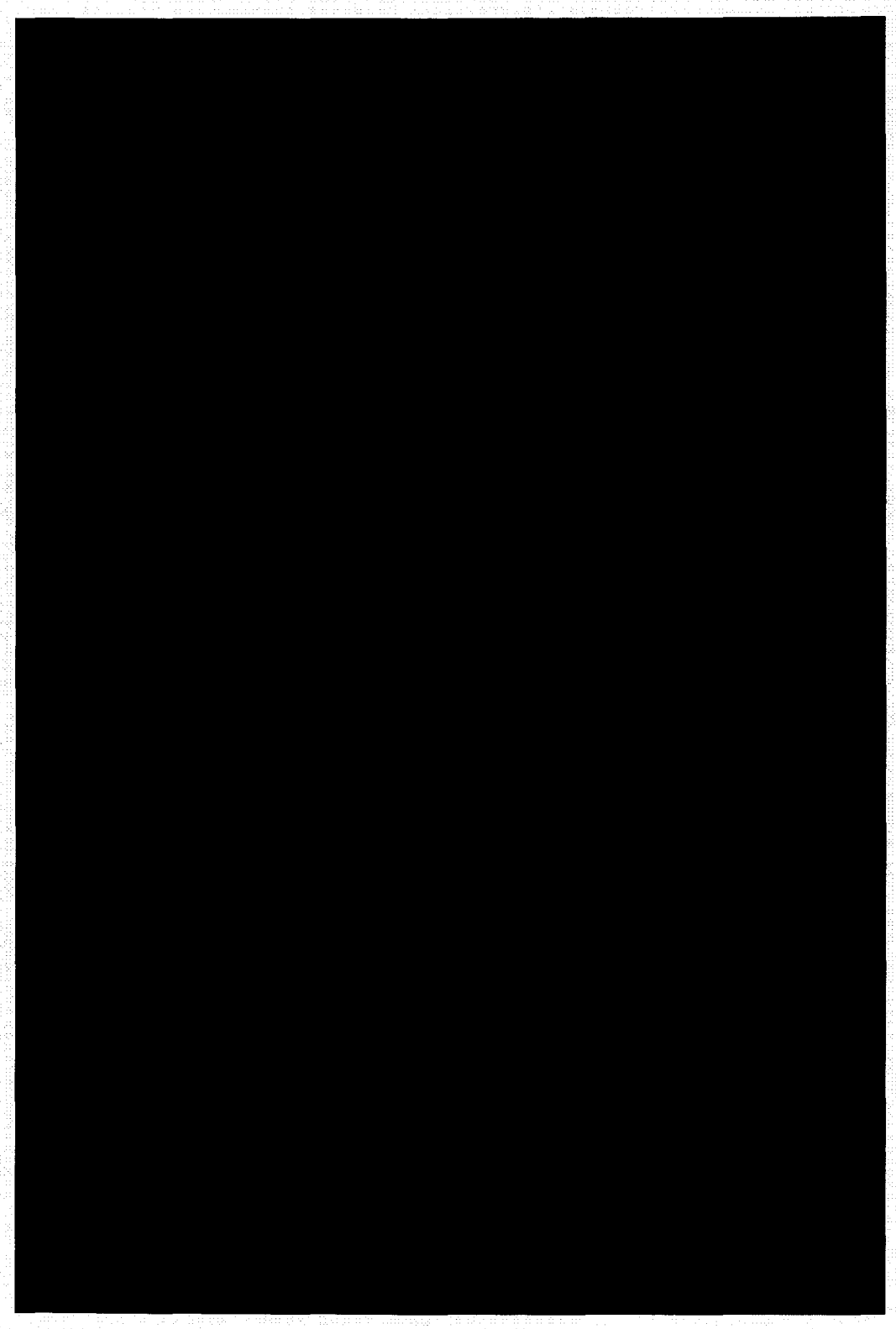
Compte tenu de ce qui précède, les présentes instructions du ministre au directeur du Service canadien de renseignement de sécurité (SCRS) énoncent, conformément au paragraphe 6(2) de la *Loi sur le SCRS*, les priorités en matière de collecte de renseignements pour l'exercice 2011-2012, lesquelles tiennent compte du mandat et des ressources du SCRS. Elles serviront également à l'élaboration des exigences en matière de renseignement du SCRS.

Ces priorités resteront en vigueur jusqu'à ce qu'elles soient renouvelées ou remplacées par le ministre.

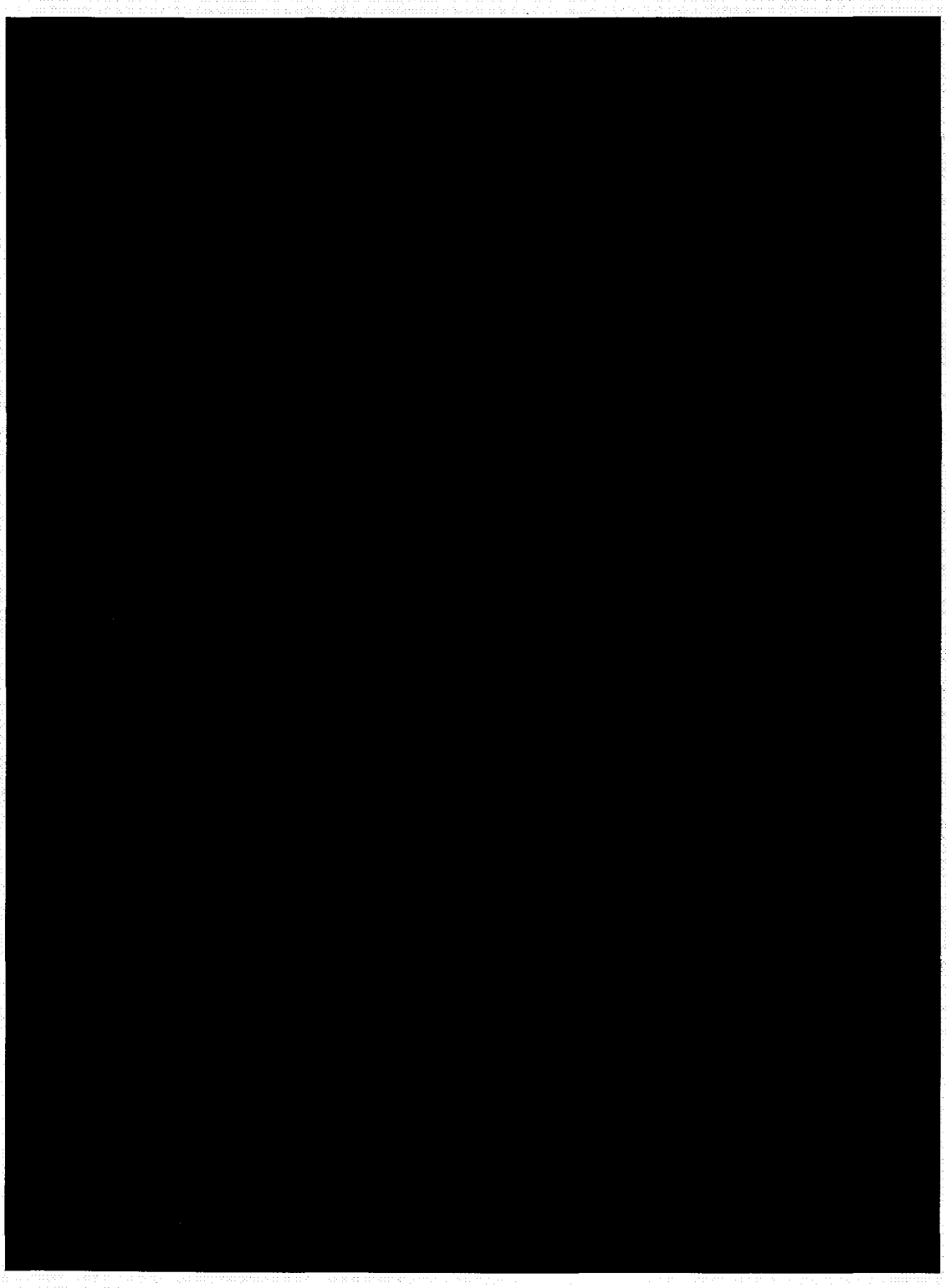
PRIORITÉS EN MATIÈRE DE RENSEIGNEMENT

De nos jours, le contexte de la menace est de plus en plus complexe, changeant et de portée internationale. Les renseignements demeurent essentiels pour lutter contre les menaces pour la sécurité du Canada que représentent des individus et des organisations ainsi que certains États, groupes terroristes et services de renseignements étrangers.

Le SCRS doit continuer de recueillir des informations et des renseignements, tant au pays qu'à l'étranger, sur les menaces pour la sécurité du Canada. Conformément aux priorités énoncées dans le présent document, le SCRS doit répondre aux besoins changeants en matière de renseignement et réagir rapidement [redacted]



[redacted]



[redacted]

[redacted]

RAPPORT AU MINISTRE

Bien que le SCRS informe constamment le gouvernement des menaces pour la sécurité du Canada, le directeur doit, dans les plus brefs délais, signaler au ministre de la Sécurité publique toute menace importante pour la sécurité du Canada ou tout risque de controverse publique associé au mandat du Service.

Pour aider à préparer le rapport sur les dépenses en matière de sécurité nationale, le SCRS doit collaborer avec les représentants de Sécurité publique Canada afin de trouver un moyen efficace de rendre compte de la répartition, en 2011-2012, des ressources affectées aux nouvelles priorités en matière de renseignement, et ce dans le but de présenter ces informations dans le rapport annuel du directeur.

[redacted]

TAB

2

[redacted]

RE / OBJET:

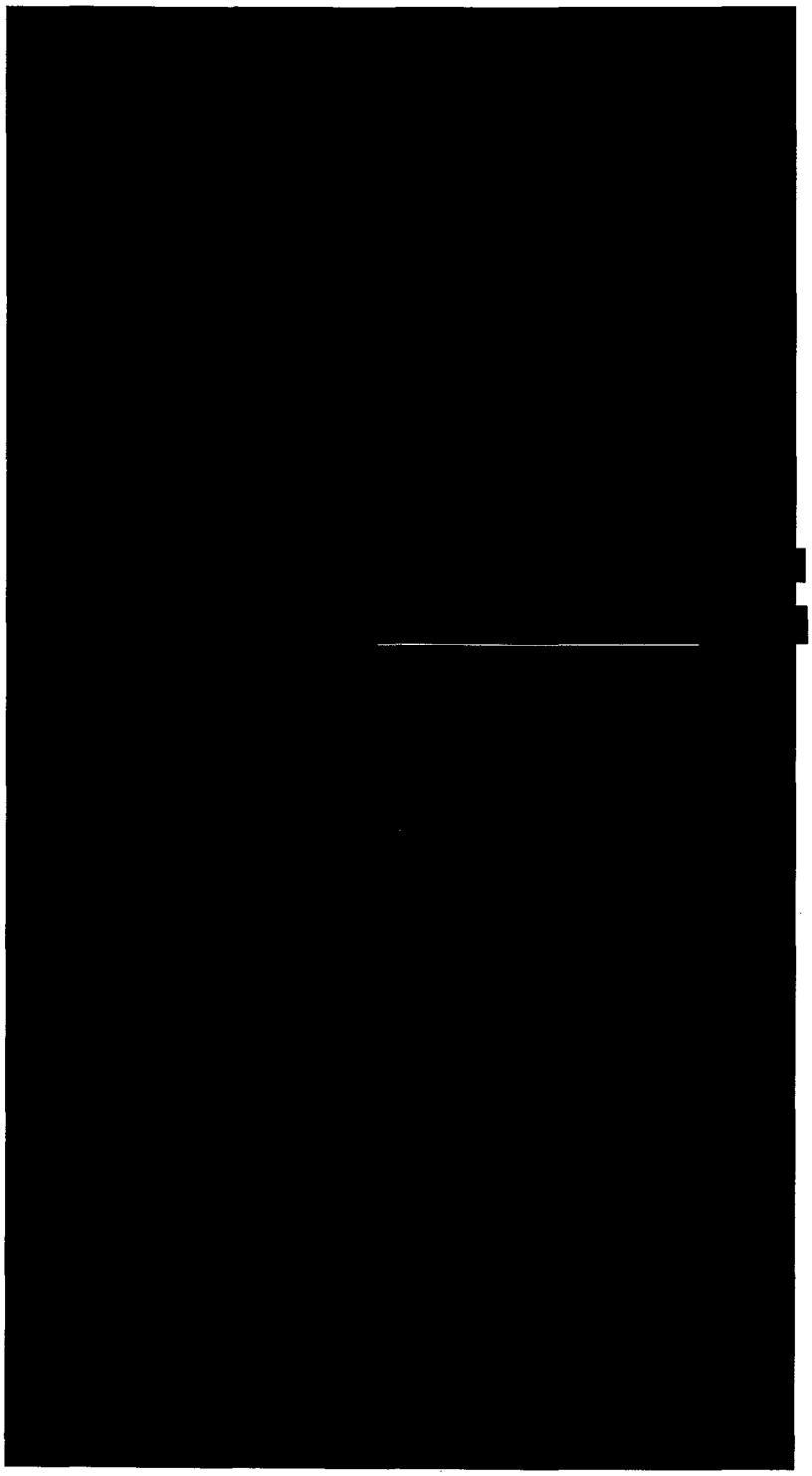
[redacted]

SYNOPSIS / SOMMAIRE:

[redacted]

[redacted]

INFORMATION / RENSEIGNEMENTS:



[redacted]

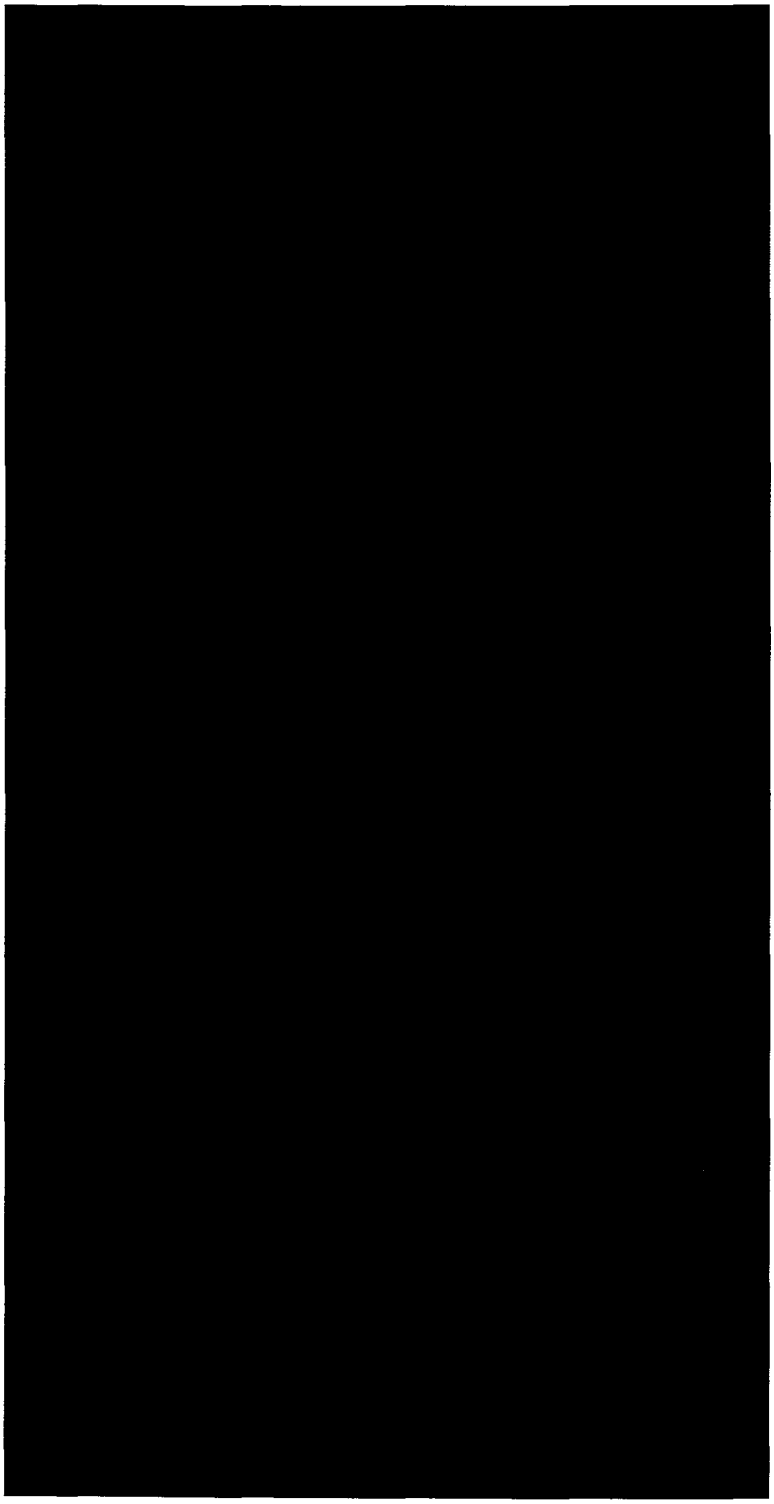
3) Emerging threats concerning the potential for serious violence related to demonstration / protest activity remains a legitimate focus of Service investigation. That said, the Service must conduct mandated investigations while still respecting, and being seen to respect, the integrity of the right to engage in legitimate protest and dissent. [redacted]

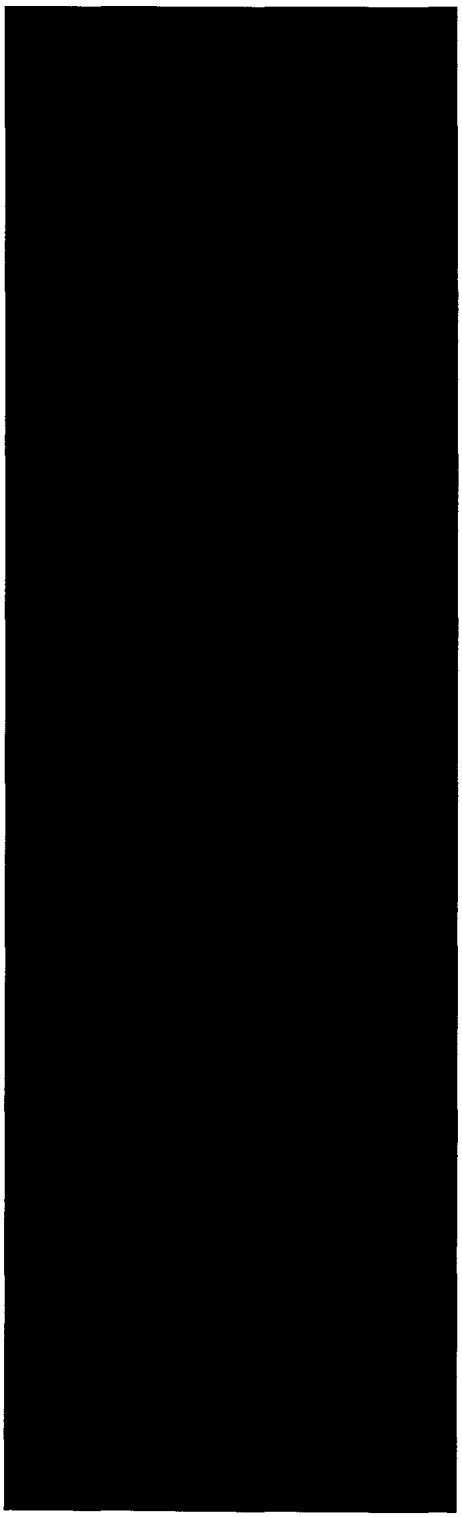
DIRECTION:

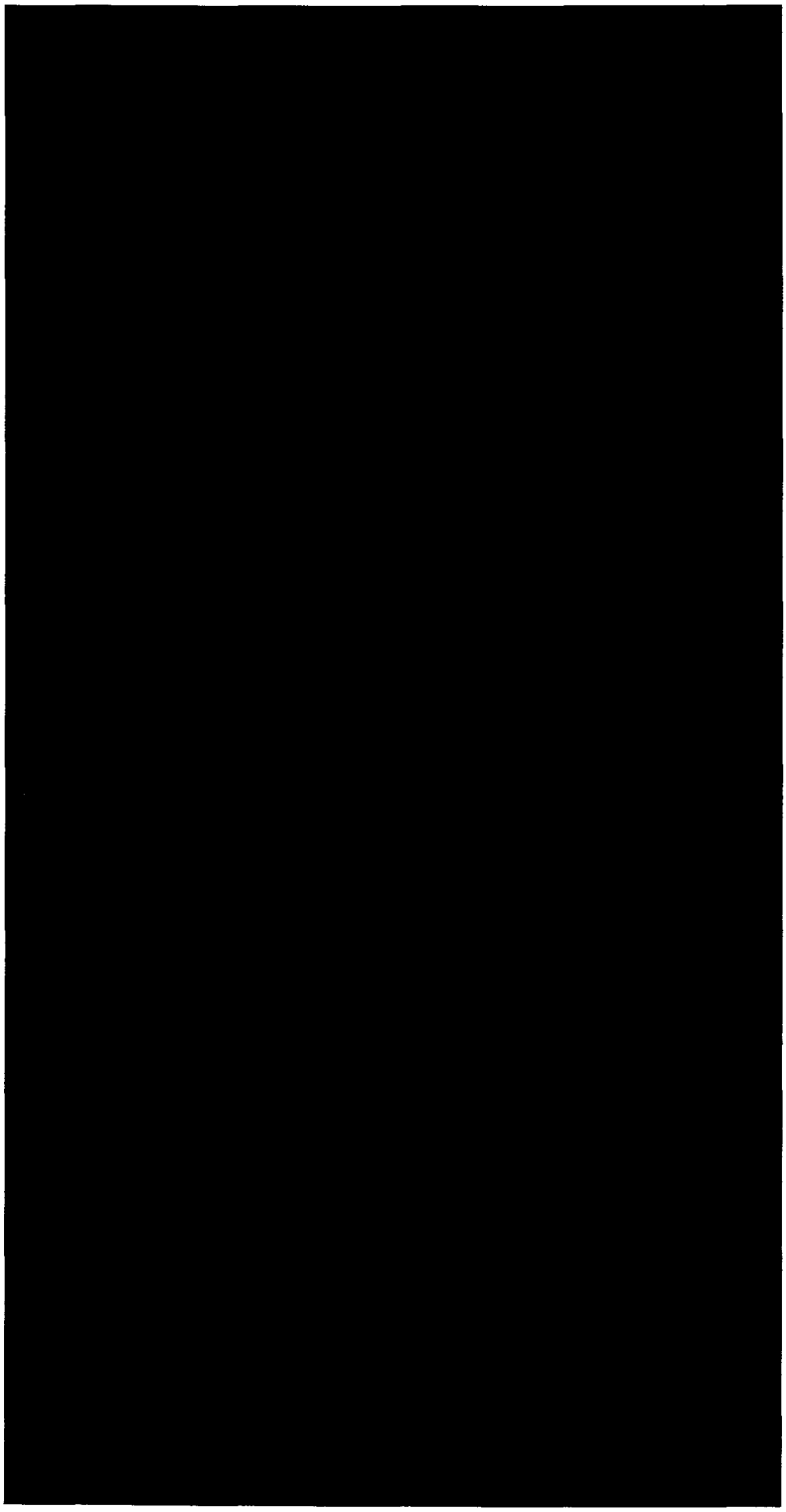
[redacted]

[redacted]

As you are aware, our focus is not on legitimate protest or dissent but rather on serious violence emanating from [redacted]







Classification: Secret
Classification : Secret
Restriction : NR / AR
File Number / No. de dossier : [redacted]

Good afternoon [redacted]

Below is an invitation for the NEB to an upcoming CSIS briefing. Could you please pass this on to Nelson Peters on behalf of IAB? We realize this may not fit into his travel schedule to Ottawa but, nevertheless, we wanted to make sure he was informed so that he can attend if he was planning to be in Ottawa at that time.

Also, if you have Nelson's open email address, could you pass that on to me?

Thank-you.

[redacted]

****

Colleagues,

On Thursday April 21, 2011 from 9:00am to 11:00am, the Government Liaison Office of the Intelligence Assessments Branch (IAB) at CSIS will host a [redacted] Briefing at CSIS National Headquarters at 1941 Ogilvie Road, Ottawa. This presentation is designed to provide an overview of [redacted] The presentation will be held at the SECRET level.

Please extend this invitation to your staff and colleagues and RSVP to the IAB - Government Liaison Office (GLO) with their full name, DOB, and security clearance by 1:00 p.m., Friday, April 15, 2011. Space is limited. The GLO can be reached at [redacted]

We look forward to your attendance and hope to see you on the 21st.

Government Liaison Office
Intelligence Assessments Branch
CSIS

Chers collègues,

Le Bureau de liaison avec le gouvernement, de la Direction de l'évaluation du renseignement (DER), du SCRS donnera un Breffage [redacted]

[redacted] le jeudi 21 avril 2011 de 9h à 11h à l'AC du SCRS, sise au 1941, chemin Ogilvie, Ottawa. Cette présentation est conçue afin de vous donner un aperçu [redacted]

[redacted] La présentation s'effectuera au niveau SECRET.

Veuillez inviter votre personnel et vos collègues, puis RSVP à la DER - Bureau de liaison avec le gouvernement; donnez le nom complet, la date de naissance et la classification de sécurité au plus tard à 13h, le vendredi 15 avril 2011. Le nombre de places est limité. Vous pouvez joindre le BLG au [redacted]

Nous espérons que vous serez des nôtres et que nous vous reverrons le 21!

Bureau de liaison avec le gouvernement
Direction de l'évaluation du renseignement
SCRS

CSIS Intelligence Assessments Branch
Government Liaison Office
[redacted]

[redacted]

Classification: Secret//Canadian Eyes Only
Classification : Secret//Réservé aux Canadiens
[redacted]

>>> [redacted] 9/7/2010 4:10 pm >>>
Classification: Secret
Classification : Secret
Not for PA / Ne pas classer

Good Afternoon All:

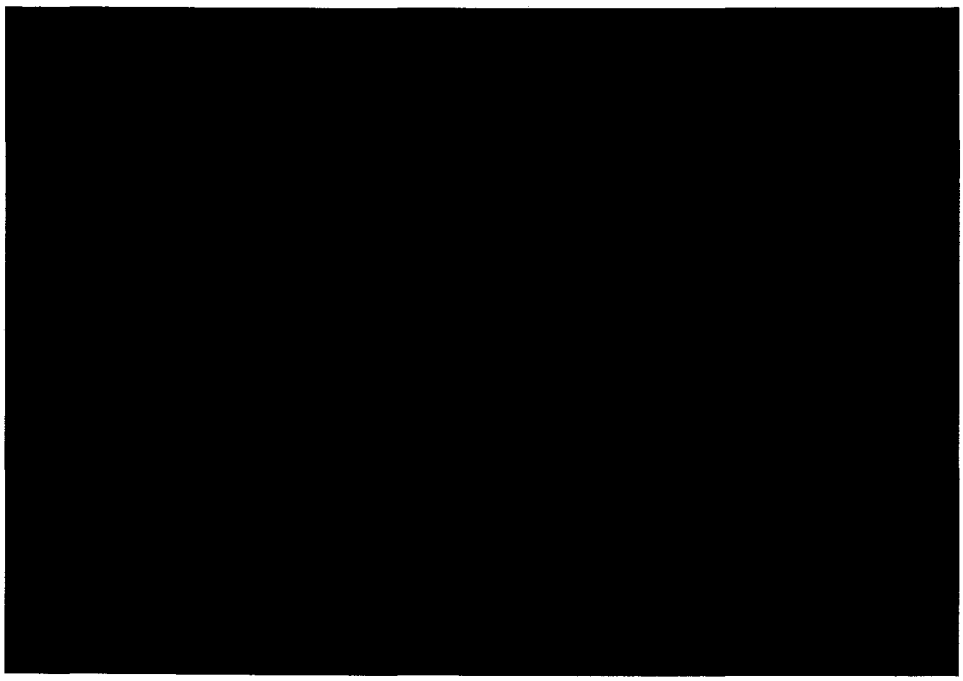
Here are the highlights from our meeting with NEB's Kevin Campbell.

Cheers,

[redacted]

[redacted]

[redacted]



Minister of Public Safety | Ministre de la Sécurité publique

AUG 04 2010

BY HAND **TOP SECRET // CEO**

Mr. Richard Fadden
Director
Canadian Security Intelligence Service
1941 Ogilvie Road
Gloucester, Ontario K1J 1B7

Dear Mr. Fadden:

Attached you will find my written Direction as per section 6(2) of the *Canadian Security Intelligence Service Act* with respect to intelligence priorities of the Service. This Ministerial Direction will replace the previous Ministerial Direction on Intelligence Priorities set out in 2009.

The new Ministerial Direction provides high-level guidance regarding intelligence priorities that were approved by the Ad Hoc Committee of Ministers on Security and Intelligence on April 19, 2010.

A copy of this letter and the enclosed Ministerial Direction will be sent to the Chair of the Security Intelligence Review Committee, and to the Inspector General of the Canadian Security Intelligence Service.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

Enclosure: (1)

CSIS / SCRS
[redacted]
AUG 10 2010
[redacted] DIR

Canada

MINISTERIAL DIRECTION TO THE DIRECTOR OF THE CANADIAN SECURITY INTELLIGENCE SERVICE: INTELLIGENCE PRIORITIES FOR 2010-2011

This Ministerial Direction provides guidance to the Director of the Canadian Security Intelligence Service (CSIS), pursuant to subsection 6(2) of the *CSIS Act*, on the Intelligence Priorities for 2010-2011. These intelligence priorities shall remain in effect until renewed or replaced by the Minister.

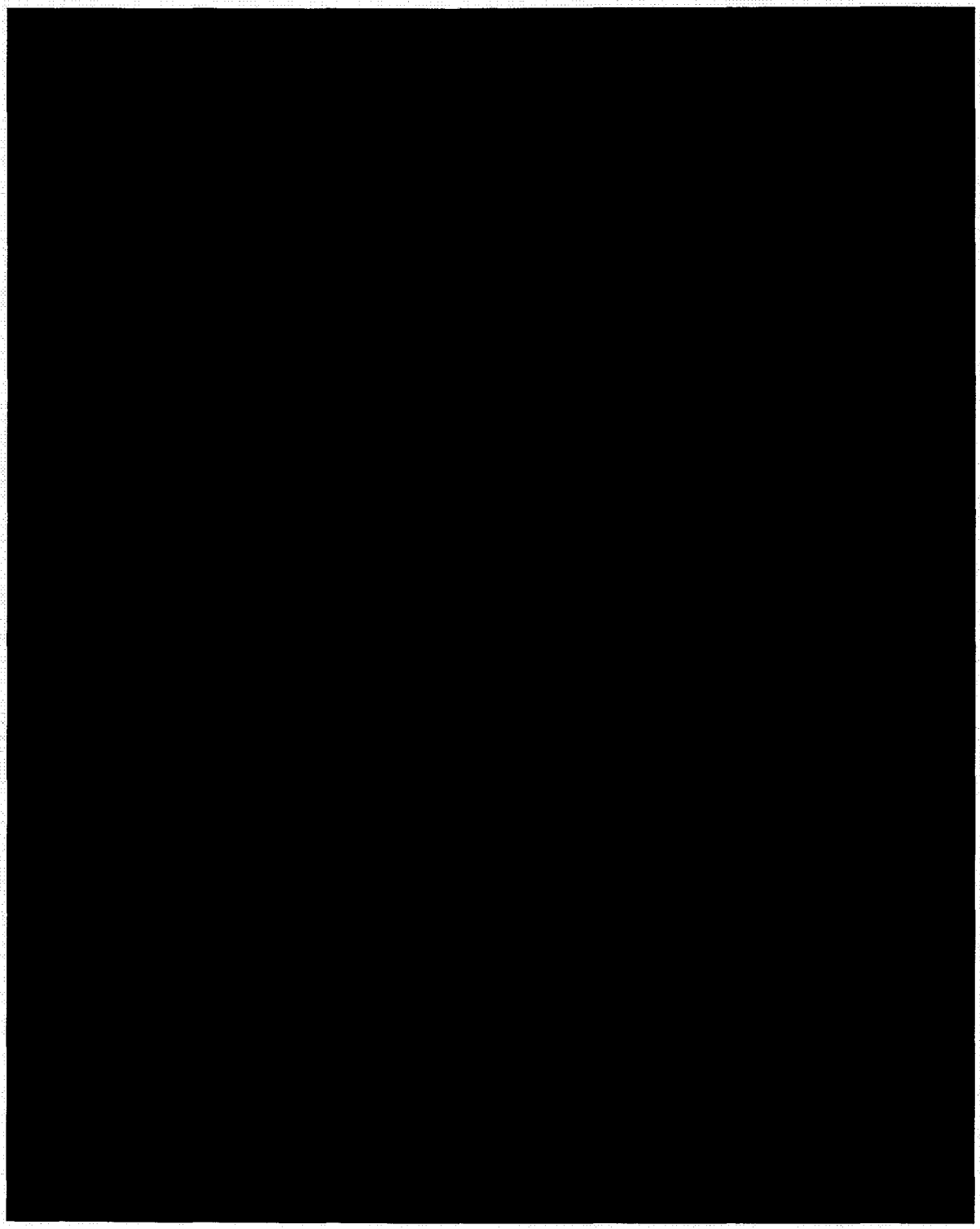
INTELLIGENCE PRIORITIES

Today's complex threat environment is increasingly global and fluid in nature, and intelligence continues to be the key to counter threats to the security of Canada posed by states, terrorist groups, foreign intelligence agencies, and other individuals and entities.

CSIS is directed to continue to collect information and intelligence both within Canada and abroad on threats to the security of Canada. Consistent with the priorities outlined herein, CSIS is directed to meet evolving intelligence needs and respond to emerging issues in a timely manner [redacted]

[redacted]

[redacted]



[redacted]

REPORTING TO THE MINISTER

Notwithstanding that CSIS advises the Government on an ongoing basis of threats to the security of Canada, the Director should report to the Minister of Public Safety, in a timely manner, on any significant risk to the security of Canada or potential for public controversy related to the Service's mandate.

INSTRUCTIONS DU MINISTRE AU DIRECTEUR DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ : PRIORITÉS EN MATIÈRE DE RENSEIGNEMENT POUR 2010-2011

Conformément au paragraphe 6(2) de la *Loi sur le Service canadien du renseignement de sécurité (SCRS)*, les présentes instructions du ministre au directeur du SCRS énoncent les priorités en matière de collecte de renseignement pour l'exercice 2010-2011. Ces priorités resteront en vigueur jusqu'à ce qu'elles soient renouvelées ou remplacées par le ministre.

PRIORITÉS EN MATIÈRE DE RENSEIGNEMENT

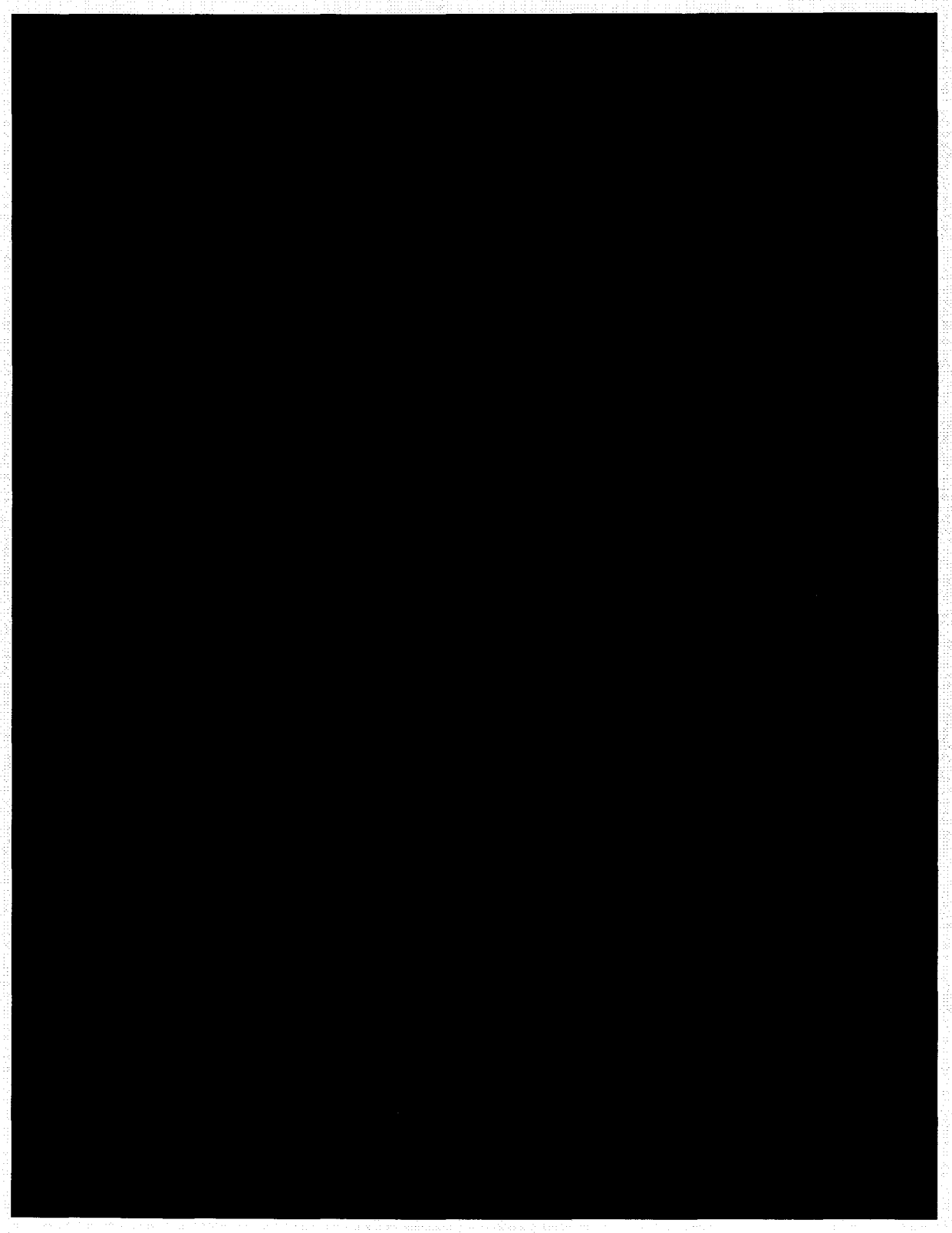
De nos jours, le contexte de la menace est complexe, souple et, par sa nature, de portée internationale. Le renseignement est un élément clé pour la lutte contre les menaces à la sécurité du Canada que posent divers États, groupes terroristes, services du renseignement étrangers et autres individus et entités.

Le SCRS se voit confier le mandat de continuer à faire enquête sur les menaces à la sécurité du Canada, tant au pays qu'à l'étranger. Conformément aux priorités énoncées ci-après, le SCRS doit s'adapter aux besoins changeants en matière de renseignement et faire rapidement [redacted]

[redacted]

[redacted]

[redacted]



[redacted]

RAPPORT AU MINISTRE

Bien que le SCRS informe régulièrement le gouvernement des menaces à la sécurité du Canada, le directeur doit, dans les plus brefs délais, signaler au ministre de la Sécurité publique toute menace importante pour la sécurité du Canada ou tout risque de controverse publique associé au mandat du Service.

OPS-101-1 PROCEDURES - TARGETING SECTION 12 - LEVEL 1

1. INTRODUCTION

Scope

1.1 To detail the process for seeking a Level 1 targeting decision.

Governing Policy

1.2 OPS-101, "Targeting Section 12 - Level 1".

2. DIRECTIVES ON LEVEL 1 TARGETING

2.1 Prior to submitting an Assessment Report, consultation between the Region(s) and the appropriate Headquarters Branch, or Branches, will take place and be documented in the Assessment Report.

2.2 Employees requesting a targeting level must complete and submit a [redacted]

2.3 Using [redacted] the employee submits any biographical data known at the time of the request, using the appropriate [redacted] and indicating the section 2, *CSIS Act*, threat paragraph reference(s).

2.3.1 Upon forwarding the [redacted] Upon receipt, all relevant data in the targeting database will be verified by the Chief, Deputy Director of Operations (DDO) Secretariat, or the person designated.

2.4 Upon receipt of the approved [redacted] by the Information Management Division (IMD) and the Chief DDO Secretariat, a file number(s) will be generated for any new target(s). Where a target has been the subject of a previous targeting level, the target's file number will continue to be used.

2.4.1 [redacted]

Composite Targeting Decisions

2.5 Where targeting decisions are required on more than one (1) individual [redacted]

2.6 The [redacted] and s.2, *CSIS Act*, threat paragraph reference(s) will be clearly noted for each individual in a composite Assessment Report.

2.7 Each individual in a composite Assessment Report must be the subject of a same Certificate.

3. NOTIFICATION

3.1 Notification of a targeting decision is submitted via [redacted] using the following [redacted] files:

[redacted]

3.1.1 All other form of correspondence related to a targeting decision must also make use of the appropriate [redacted] file.

3.2 The Chief, DDO Secretariat will be notified of a targeting decision by the Targeting Coordinator of the approving authority and will amend the records held in the targeting database accordingly.

3.3 When a targeting decision is made, the requesting employee must notify:

a) IMD, Information Management / Information Technology Branch (IM/IT);

b) the appropriate Headquarters (HQ) Branch or Branches;

c) the appropriate regional operational desk(s);

d) the Chief DDO Secretariat via the [redacted] of the DDO Secretariat; and

e) the HQ and regional Targeting Coordinators (if applicable).

3.4 When responsibility for an active target is transferred from one Region or HQ Branch to another, the Region or HQ Branch assuming this responsibility will notify the [redacted] of the DDO Secretariat, via email, of the effective date of the transfer.

4. RENEWAL

4.1 An employee may renew a Level 1 due to expire by submitting an Assessment Report approved by the Regional Director General (RDG) or HQ Director General (DG), via [redacted] BRS. Refer to OPS-100-1, "Procedures - Targeting - Assessment Reports".

4.2 Targeting database updates must be done by the Chief DDO Secretariat for those renewals submitted via [redacted]

Downgrading of a Level 2

4.3 An existing Level 2 can be renewed as a Level 1(downgrade) when the Level 2 collection techniques are no longer justifiable and a Level 1 is sufficient to continue collecting information on the threat.

Upgrading to a Level 2

4.4 An existing Level 1 can be renewed as a Level 2 (upgrade) when it is determined that Level 1 collection techniques are insufficient to continue collecting information on the threat.

Certificate related Targets

4.5 Where a Level 1 or Level 2 Certificate is to be renewed and there are associated individuals whose targeting level bears its expiry date, the respective RDG or HQ DG has a sixty (60) day extension to make a targeting decision on these individuals. The expiry dates of these targeting levels will be adjusted to coincide with the renewed Certificate.

5. TERMINATION

5.1 A request for termination can be made at any point during the time period granted for a Level 1.

5.2 An employee may request the termination of a Level 1 by submitting an Assessment Report approved by the RDG or HQ DG, via [redacted] to BRS. Refer to OPS-100-1, "Procedures - Targeting - Assessment Reports".

5.3 Where targeting levels of individuals are to be terminated or allowed to expire, an Assessment Report for each will be submitted.

5.4 Unless there are exceptional circumstances, an Assessment Report must be submitted via [redacted] within sixty (60) days of termination / expiration of the targeting decision, unless granted a 60 days extension by the Chief DDO Secretariat, in which case the Assessment Report must be submitted within the extension period.

OPS-102-1 PROCEDURES - TARGETING SECTION 12 - LEVEL 2

1. INTRODUCTION

Scope

1.1 To detail the process for seeking a Level 2 targeting decision.

Governing Policy

1.2 OPS-102, "Targeting Section 12 - Level 2".

2. DIRECTIVES ON LEVEL 2 TARGETING

2.1 Prior to submitting an Assessment Report, consultation between the Region(s) and the appropriate Headquarters Branch, or Branches, will take place and be documented in the Assessment Report.

2.2 Employees requesting a targeting level must complete and submit a [redacted]

2.3 Using [redacted] the employee submits any biographical data known at the time of the request, using the appropriate [redacted] and indicating the section 2, *CSIS Act*, threat paragraph reference(s).

2.3.1 Upon forwarding the [redacted] data will be automatically entered into, and be retrievable [redacted] Upon receipt, all relevant data in the targeting database will be verified by the Chief, DDO Secretariat, or the person designated.

2.4 Upon receipt of the approved [redacted] by the Information Management Division (IMD) and the Chief DDO Secretariat, a file number(s) will be generated for any new target(s). Where a target has been the subject of a previous targeting level, the target's file number will continue to be used.

2.4.1 [redacted]

Composite Targeting Decisions

2.5 Where targeting decisions are required on more than one (1) individual, [redacted]

2.6 The [redacted] and s.2, *CSIS Act*, threat paragraph reference(s) will be clearly noted for each individual in a composite Assessment Report.

2.7 Each individual in a composite Assessment Report must be the subject of a same Certificate.

3. NOTIFICATION

3.1 Notification of a targeting decision is submitted via [redacted] using the following [redacted] files:

[redacted]

3.1.1 All other form of correspondence related to a targeting decision must also make use of the appropriate [redacted] file.

3.2 The Chief, DDO Secretariat will be notified of a targeting decision by the Targeting Coordinator of the approving authority and will amend the records held in the targeting database accordingly.

3.3 When a targeting decision is made, the requesting employee must notify:

a) IMD, Information Management / Information Technology Branch (IM/IT);

b) the appropriate Headquarters (HQ) Branch or Branches;

c) the appropriate regional operational desk(s);

d) via the [redacted] of the DDO Secretariat, the Chief DDO Secretariat; and

e) the HQ and regional Targeting Coordinators (if applicable).

3.4 When responsibility for an active target is transferred from one Region or HQ Branch to another, the Region or HQ Branch assuming this responsibility will notify the [redacted] of the DDO Secretariat, via email, of the effective date of the transfer.

4. RENEWAL

4.1 An employee may renew a Level 2 due to expire by submitting an Assessment Report approved by the Regional Director General (RDG) or HQ Director General (DG), via [redacted] to BRS. Refer to OPS-100-1, "Procedures - Targeting - Assessment Reports".

4.2 Targeting database updates must be done by the Chief DDO Secretariat for those renewals submitted via [redacted]

Downgrading of a Level 2

4.3 An existing Level 2 can be renewed as a Level 1(downgrade) when the Level 2 collection techniques are no longer justifiable and a Level 1 is sufficient to continue collecting information on the threat.

Upgrading of a Level 1

4.4 An existing Level 1 can be renewed as a Level 2 (upgrade) when it is determined that Level 1 collection techniques are insufficient to continue collecting information on the threat.

Certificate related Targets

4.5 Where a Level 1 or Level 2 Certificate is to be renewed and there are associated individuals whose targeting level bears its expiry date, the respective RDG or HQ DG has a sixty (60) day extension to make a targeting decision on these individuals. The expiry dates of these targeting levels will be adjusted to coincide with the renewed Certificate.

5. TERMINATION

5.1 A request for termination can be made at any point during the time period granted for a Level 2.

5.2 An employee may request the termination of a Level 2 by submitting an Assessment Report approved by the RDG or HQ DG, via [redacted], to BRS. Refer to OPS-100-1, "Procedures - Targeting - Assessment Reports".

5.3 Where targeting levels of individuals are to be terminated or allowed to expire, an Assessment Report for each will be submitted.

5.4 Unless there are exceptional circumstances, an Assessment Report must be submitted via [redacted] within sixty (60) days of termination / expiration of the targeting decision, unless granted a 60 days extension by the Chief DDO Secretariat, in which case the Assessment Report must be submitted within the extension period.

TAB

7

[redacted]

DATE
20100204

[redacted]

RE / OBJET:

[redacted]

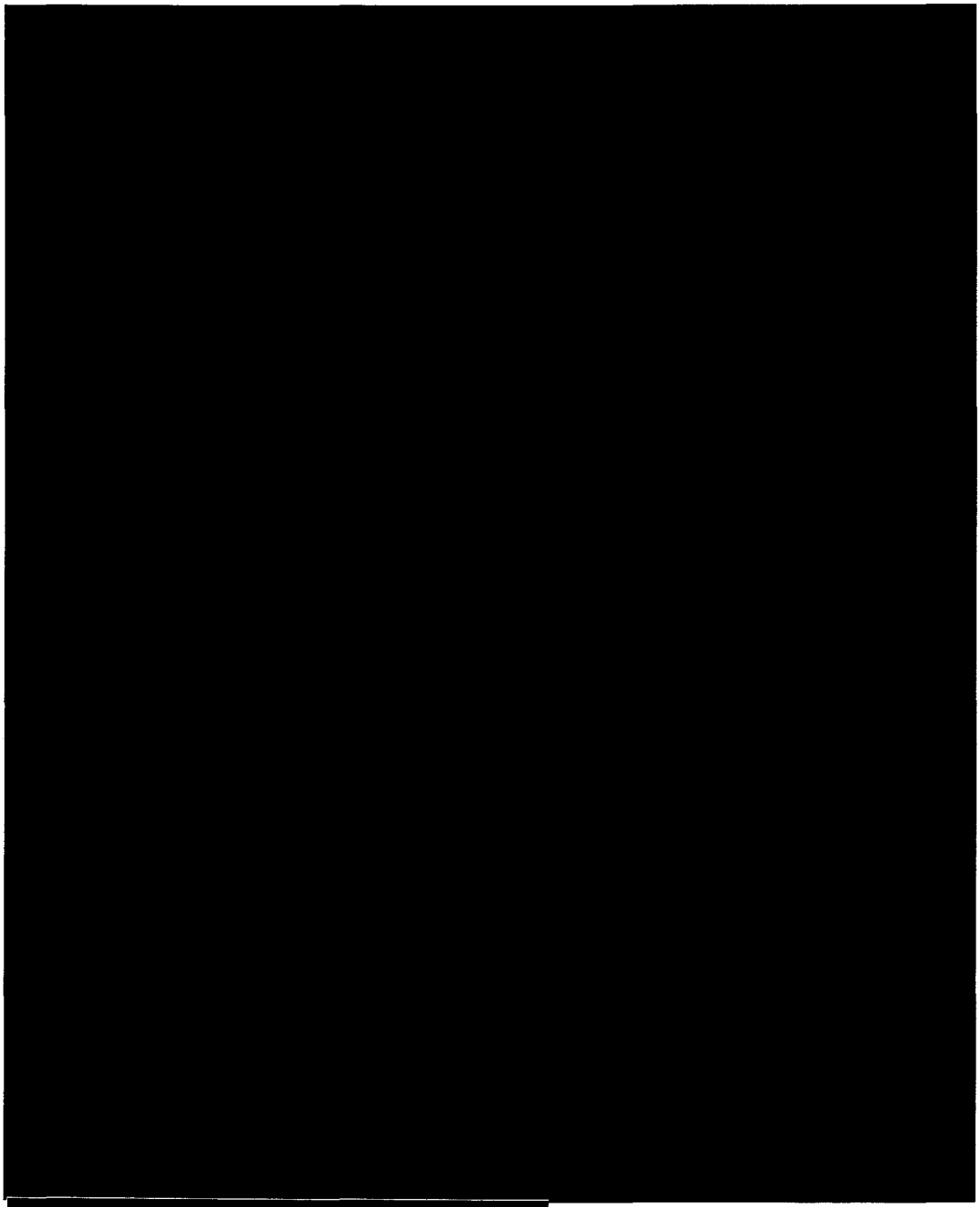
SYNOPSIS / SOMMAIRE:

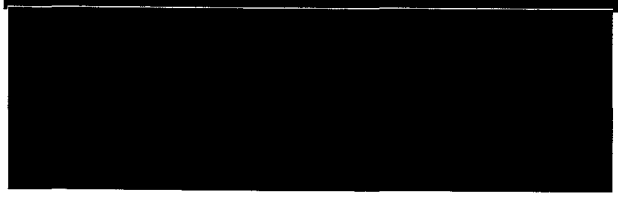
[redacted]

INFORMATION / RENSEIGNEMENTS:

[redacted]

[redacted]





Minister of Public Safety | Ministre de la Sécurité publique

JUN 18 2009

BY HAND **TOP SECRET / CEO**

Mr. Jim Judd
Director
Canadian Security Intelligence Service
1941 Ogilvie Road
Ottawa, Ontario K1J 1B7

CSIS/SCRS
JUN 2 2 2009
[redacted]

Dear Mr. Judd,

Attached you will find my written Direction as per section 6(2) of the *Canadian Security Intelligence Service Act* with respect to intelligence priorities of the Service. This Direction will replace the previous Ministerial Direction on Intelligence Priorities set out in 2008.

The new Ministerial Direction provides high-level guidance regarding intelligence priorities that were approved by the Ad Hoc Committee of Ministers on Security and Intelligence on April 07, 2009.

A copy of this letter and the enclosed Ministerial Direction will be sent to the Chair of the Security Intelligence Review Committee, and to the Inspector General of the Canadian Security Intelligence Service.

Yours sincerely,

Peter Van Loan, P.C., M.P.
Minister of Public Safety

Enclosure (1)

2009-07-07
[redacted]
580-0-40

Canada

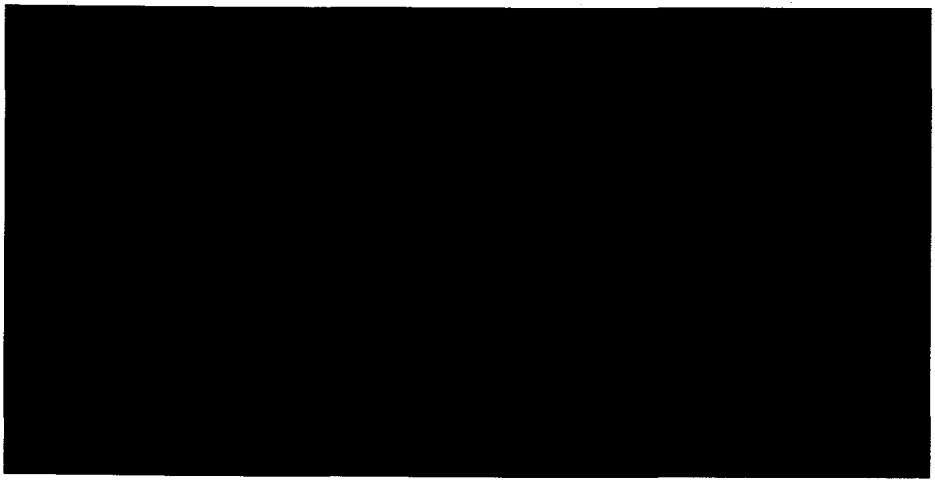
MINISTERIAL DIRECTION TO THE DIRECTOR,
CANADIAN SECURITY INTELLIGENCE SERVICE:
INTELLIGENCE PRIORITIES FOR 2009-2010

This Ministerial Direction provides guidance to the Director of the Canadian Security Intelligence Service (CSIS), pursuant to subsection 6(2) of the *CSIS Act*, on the Intelligence Priorities for fiscal year 2009-2010. These intelligence collection priorities shall remain in effect until renewed or replaced by the Minister.

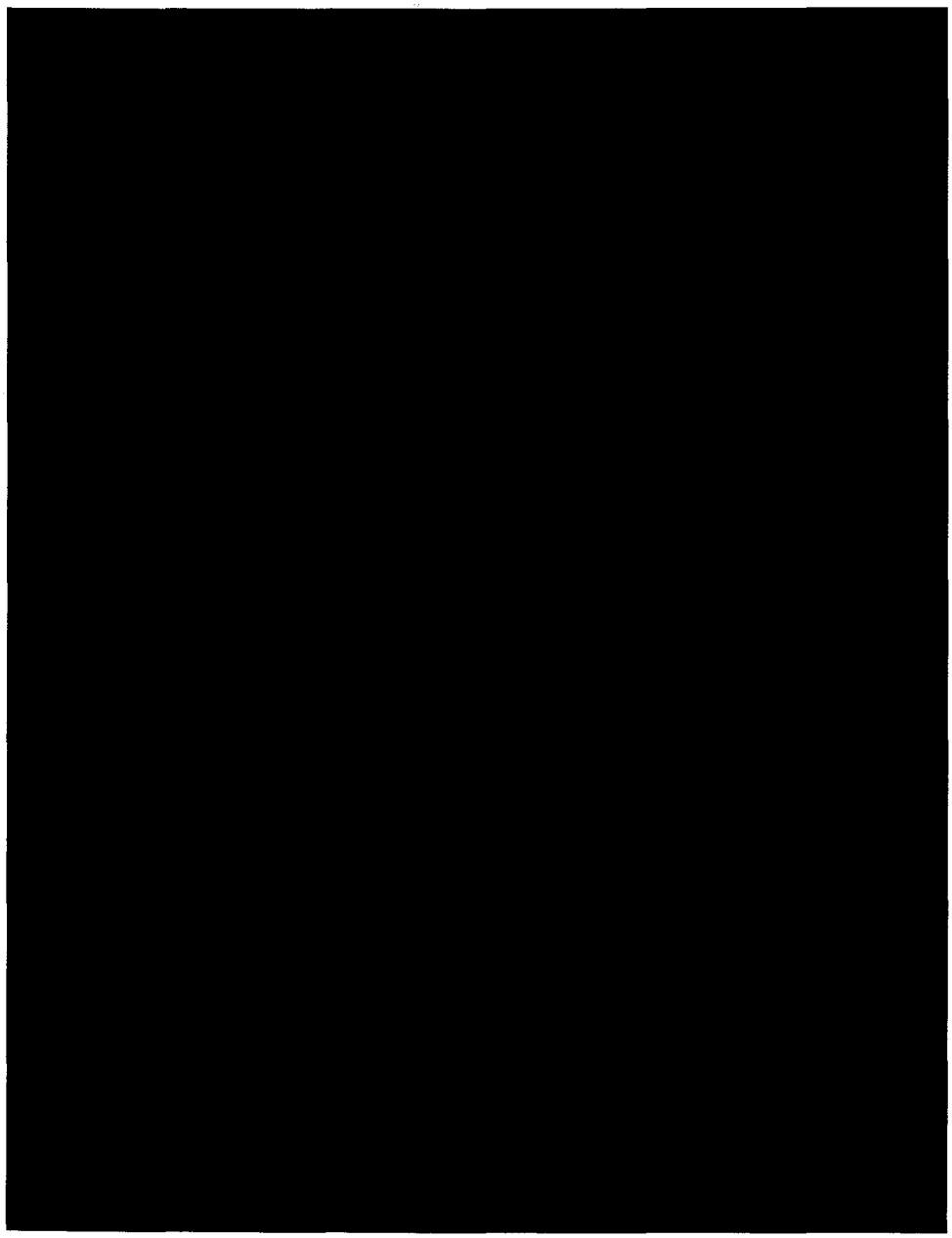
INTELLIGENCE PRIORITIES

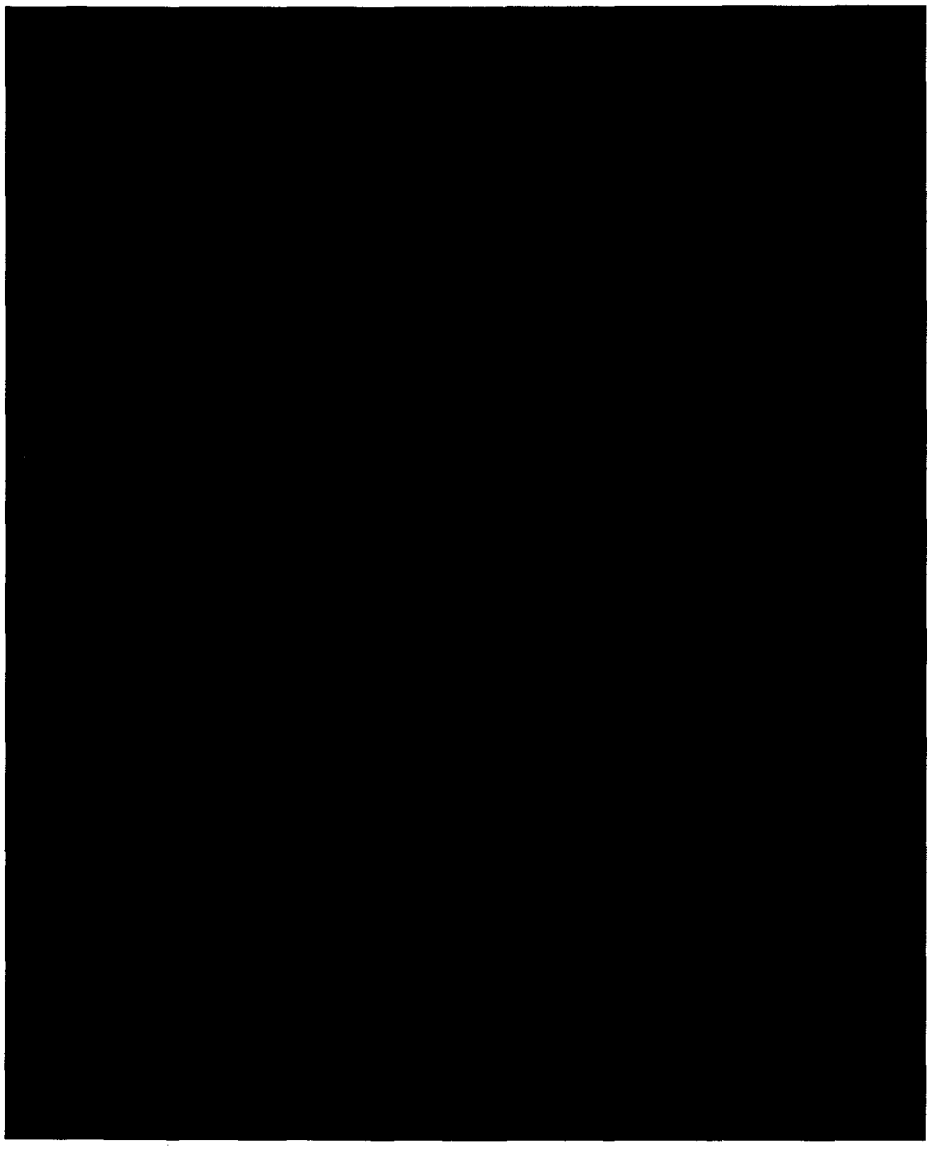
Today's complex threat environment is increasingly global in nature, and intelligence continues to be the key to counter threats to the security of Canada posed by states, terrorist groups, criminals, foreign intelligence agencies, and other individuals and entities.

CSIS is directed to continue to investigate threats to the security of Canada both within Canada and abroad. Consistent with the priorities outlined herein, CSIS is directed to meet evolving intelligence needs through reliance on risk management and flexibility to concentrate resources on the foremost threats, while ensuring that it can respond to emerging issues in a timely manner.



1/4





[redacted]

The 2010 Vancouver Winter Olympic Games

The Vancouver 2010 Winter Olympic Games will be a high-profile international event which will focus global attention on Canada. [redacted]

[redacted] with the 2010 Vancouver Winter Olympic Games including ongoing security preparations for the 2010 G8 Summit.

[redacted]

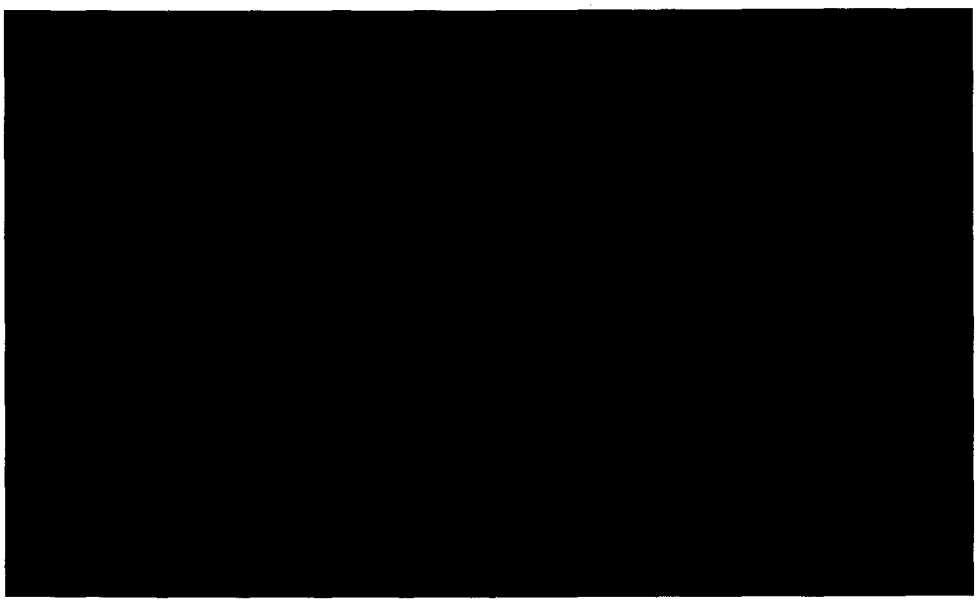
INSTRUCTIONS DU MINISTRE AU DIRECTEUR DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ : PRIORITÉS EN MATIÈRE DE RENSEIGNEMENT POUR 2009-2010

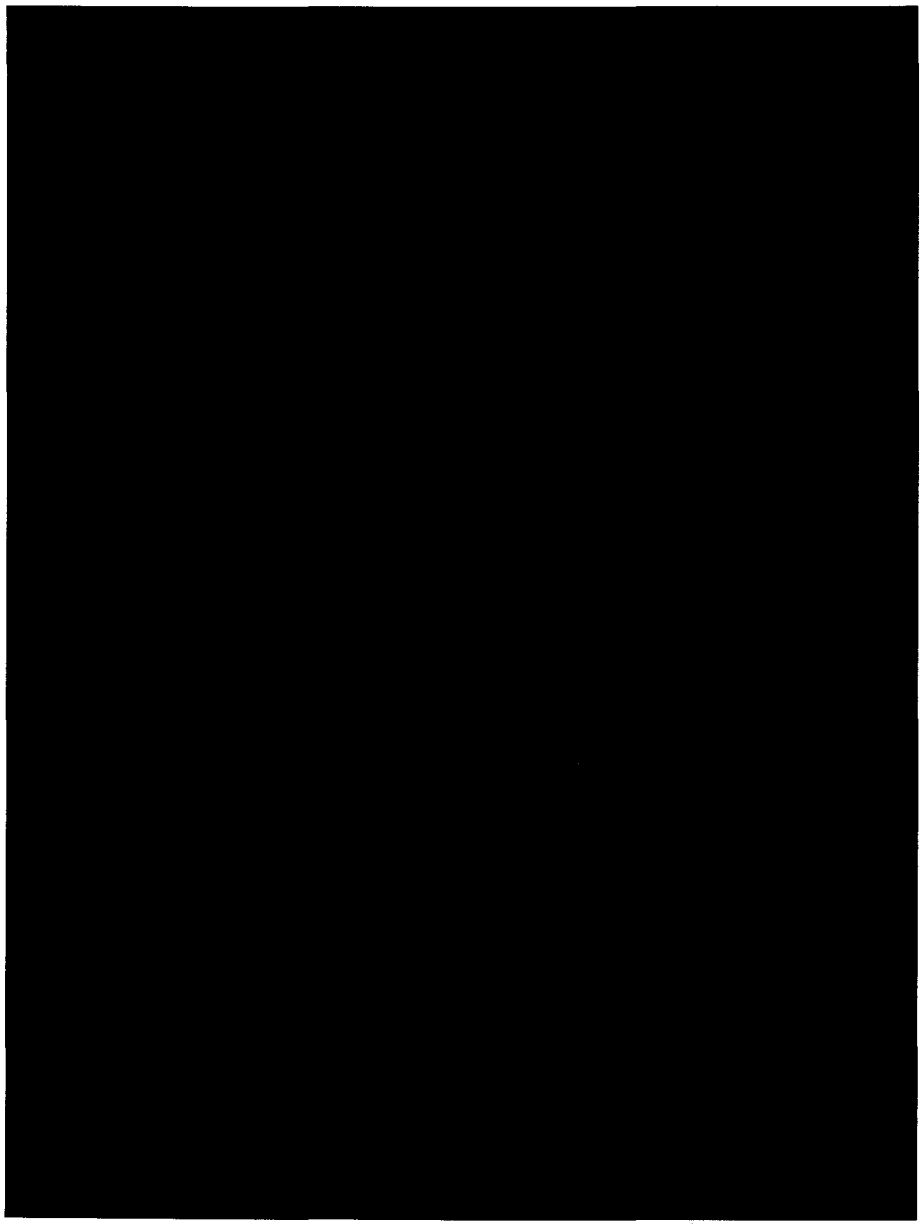
Conformément au paragraphe 6(2) de la *Loi sur le Service canadien du renseignement de sécurité (SCRS)*, les présentes instructions du ministre au directeur du SCRS énoncent les priorités en matière de collecte de renseignement pour l'exercice 2009-2010. Ces priorités resteront en vigueur jusqu'à ce qu'elles soient renouvelées ou remplacées par le ministre.

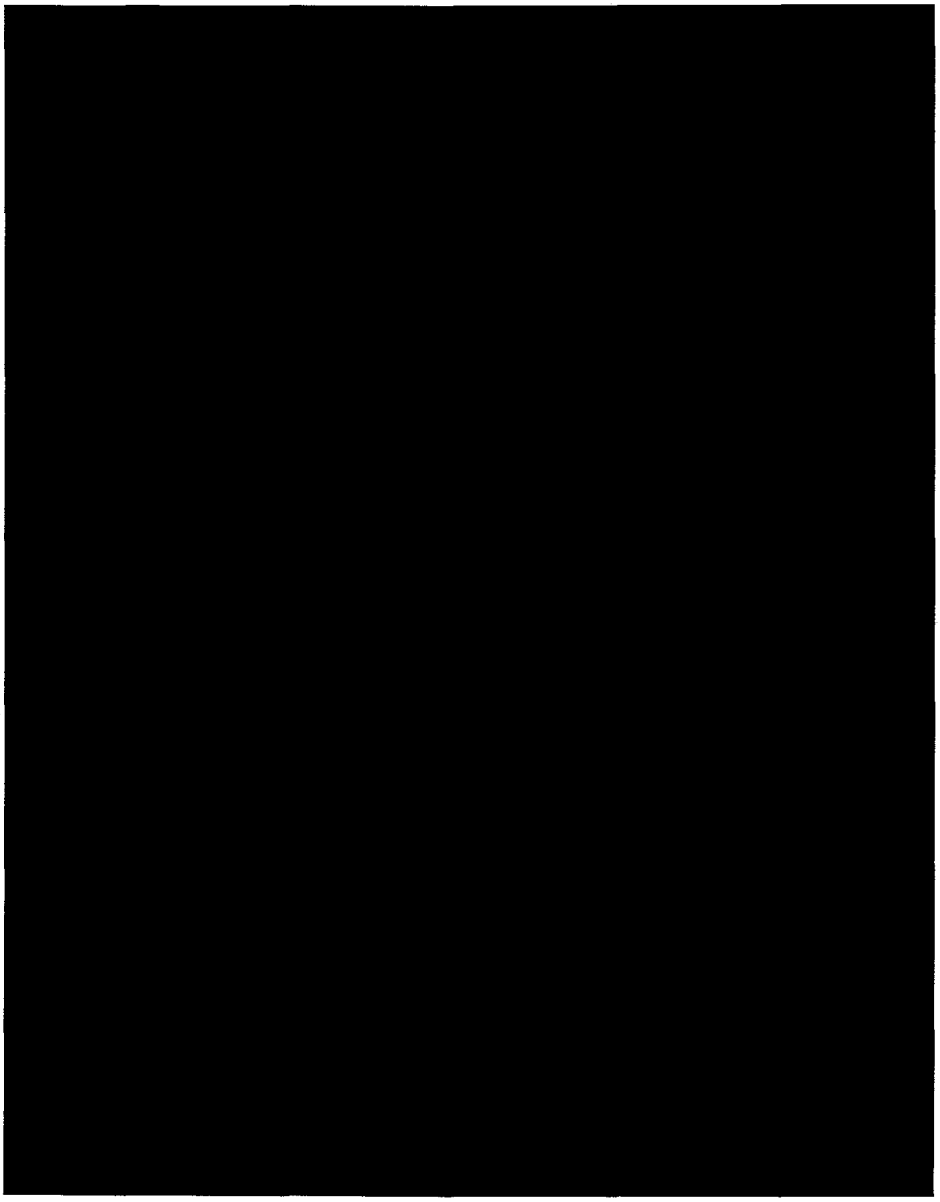
PRIORITÉS EN MATIÈRE DE RENSEIGNEMENT

De nos jours, le contexte de la menace est complexe et, par sa nature, de portée internationale. Le renseignement est un élément clé pour la lutte contre les menaces à la sécurité du Canada que posent divers États, groupes terroristes, criminels, organismes du renseignement étrangers et autres individus et entités.

Le SCRS a pour mandat de continuer à faire enquête sur les menaces à la sécurité du Canada, tant au pays qu'à l'étranger. Conformément aux priorités énoncées ci-après, le SCRS doit répondre aux besoins changeants en matière de renseignement en assurant la gestion du risque et en faisant preuve de souplesse pour concentrer ses ressources sur les principales menaces tout en s'assurant d'être en mesure de réagir rapidement aux nouvelles menaces.







[redacted]

Jeux olympiques d'hiver de 2010 à Vancouver

Les Jeux olympiques d'hiver de 2010 à Vancouver seront un événement international très médiatisé qui attirera l'attention du monde entier. [redacted]

[redacted]

[redacted]

aux Jeux olympiques d'hiver de 2010 à Vancouver ainsi que ses préparatifs de sécurité en vue du Sommet du G8 de 2010.

[redacted]

[redacted]

2007-04-01
OPS-100 TARGETING - SECTION 12 CSIS ACT

1. INTRODUCTION

1.1 The Targeting Policy is established under the authority of the Director pursuant to subsection 6(1), *CSIS Act*, and directs the Service's targeting approval process.

Objective

1.2 To detail the targeting approval process to collect of information and intelligence by investigation or otherwise pursuant to section 12, *CSIS Act*.

Scope

1.3 This policy outlines the principles, as well as the organizational and functional responsibilities, pertaining to targeting.

1.4 Further to a Memorandum from Cabinet of national intelligence collection priorities the Minister of Public Safety issues a Ministerial Directive outlining general collection requirements. The Deputy Director of Operations (DDO) then provides a strategic directive to operationalize the Ministerial Directive.

Authorities and References

1.5 *Canadian Security Intelligence Service Act*

1.6 *Anti-terrorism Act*

1.7 Ministerial Direction on CSIS Operations (2001 03 01)

1.8 OPS-201, "Conduct of Operations - General"

1.9 OPS-204 to OPS-208, "Human Sources" policies

1.10 OPS-209, "Warrant Acquisition - Section 12"

1.11 OPS-210, "Execution of Warrant Powers - Section 12"

1.12 OPS-302, "Use of the Polygraph for CSIS Operations"

1.13 OPS-401, "Operational Cooperation in Canada with Domestic Government Institutions"

1.14 OPS-402, "Section 17 Arrangements with Foreign Governments and Institutions"

1.15 OPS-403, "Foreign Liaison and Cooperation"

1.16 OPS-501, "Operational Reporting"

1.17 OPS-505, "Threat Assessments"

1.18 OPS-601 to OPS-603, "Authorized Disclosure of Operational Information and Intelligence "

1.19 CSIS Operational Message System (COMS) User Manual

Definitions and Interpretations

1.20 See Appendix 1 - Definitions and Interpretations

2. PRINCIPLES

2.1 Targeting will comply with the following fundamental principles:

i) the rule of law must be observed;

ii) the investigative means must be proportional to the gravity and imminence of the threat;

iii) the need to use intrusive investigative techniques must be weighed against possible damage to civil liberties or to fundamental societal institutions;

iv) the more intrusive the investigative technique, the higher the authority required to approve its use;

v) the least intrusive investigative methods must be used first, except in emergency situations or where less intrusive investigative techniques would not be proportionate to the gravity and imminence of the threat; and

vi) lawful advocacy, protest or dissent may not be investigated unless such activities are carried out in conjunction with threats as defined in s. 2, *CSIS Act*.

3. RESPONSIBILITIES

Director

3.1 The Director is responsible for:

i) reporting to the Minister of Public Safety where there is a well founded risk of serious violence or potential public controversy relating to a mandated threat.

Deputy Director Operations

3.2 The Deputy Director Operations (DDO) or designate is responsible for:

i) managing the application of this policy and providing direction to resolve issues arising from its implementation;

ii) ensuring that targeting approvals are consistent with the Service's mandate and policies, and current intelligence requirements of the government;

iii) appointing the Chief DDO Secretariat.

Chief DDO Secretariat

3.3 The Chief DDO Secretariat is responsible for:

i) providing the DDO, Assistant Director Operations (ADO) and Assistant Director, Legal Services, within five working days from the date of approval, written confirmation of all targeting decisions taken pursuant to this policy;

ii) updating the targeting database within three working days from the receipt of a notification of targeting approval from a region or HQ branch;

iii) maintaining the targeting database including all active and inactive targeting approvals;

iv) providing advice and guidance to the Targeting Coordinators in HQ and the regions to ensure the consistent application of the targeting policy;

v) providing Security Screening Branch, on a regular basis, an updated list of targeting approvals;

vi) maintaining statistical information and produces, on request, reports of Service investigations; and

vii) performing other administrative functions as directed by the DDO or designate.

Directors General

3.4 Headquarters Operational Branch and Regional Directors General are responsible for:

i) ensuring that targeting approvals are consistent with the Service's mandate and policies, and current intelligence requirements of the government;

ii) assessing the reliability of the information supporting the request; and

iii) assessing the implications, magnitude, seriousness and immediacy of the activities suspected of constituting the threat.

3.5 The Director General of each region and of each operational branch in HQ is responsible for the appointment of a Targeting Coordinator.

4. TARGETS OF THE SERVICE

4.1 Information from a foreign state or agency may be used when submitting an application for any investigation, taking into consideration the human rights record of that foreign state or agency.

Persons

4.2 A targeting level may be approved to investigate the activities of persons who may on reasonable grounds be suspected of constituting a threat to the security of Canada pursuant to s. 2, *CSIS Act*.

Groups and Organizations

4.3 A targeting level may be approved to investigate the activities of a group of persons or an organization, including its general membership, where there are reasonable grounds to suspect:

i) the objectives or activities of the group or organization constitute a threat to the security of Canada; and

ii) participants in the group or organization understand and sympathize with threat-related objectives or activities.

4.3.1 Investigations of groups or organizations may be used to determine:

i) the elements, structure, policies or plans of a group or organization as they may relate to threats to Canadian security; and

ii) a person's relationship with, or role within, a group or organization. Once a determination has been made that a person is involved in a threat-related activity and that further investigation pursuant to s. 12, *CSIS Act*, is deemed necessary, a request for targeting approval will be submitted on the person and approved before commencing the investigation.

Issues or Events

4.4 A targeting level may be approved to investigate the activities associated with an issue or event in relation to which the Service has reasonable grounds to suspect these activities constitute a threat to the security of Canada.

4.4.1 As soon as a person or persons, groups or organizations are identified as participating in threat-related activities associated to an issue or event, a separate targeting approval will be obtained.

5. EXCLUSIONS

5.1 The following activities do not require targeting approval:

i) collection of incidental information (spin-off) which may be disclosed pursuant to subsection 19.2(a) to (d), *CSIS Act*;

ii) collection of information pursuant to s.15 and 16, *CSIS Act*;

iii) [redacted]

iv) [redacted]

v) internal investigations pursuant to s. 8 and s. 20, *CSIS Act*;

vi) research and use of internal records and databases;

vii) research and use of open information;

viii) collection and reporting of unsolicited information;

ix) placement of individuals on watch lists, e.g. the Citizenship and Immigration Canada Enforcement Information Index (EII); and

[redacted]

7. COOPERATION WITH DOMESTIC OR FOREIGN AGENCIES

7.1 Investigation by the Service pursuant to s.12, *CSIS Act*, in cooperation with a Canadian federal, provincial or territorial government department, a Canadian law enforcement authority, or a foreign police, security or intelligence organization, will only be undertaken when approved under the terms of this policy.

7.1.1 The investigations described above will be in compliance with all other Service policies.

2006-05-01
OPS-601 AUTHORIZED DISCLOSURE OF OPERATIONAL INFORMATION AND INTELLIGENCE - GENERAL

1. INTRODUCTION

Objective

1.1 The primary mandate of the Service is to report to and advise the Government regarding threats to the security of Canada. This entails the disclosure of information and intelligence by the Service to various recipients in order to fulfil its duties and functions.

1.2 The flow of information or intelligence must be controlled to protect the rights of individuals and protect the security of the Service's operations therefore disclosures are made in compliance with the *CSIS Act*, Ministerial Direction, the Government Security Policy (GSP) and other relevant legislation.

Scope

1.3 This policy prescribes the general policy and guidelines for the disclosure of operational information and intelligence and of incidental information collected by the Service in compliance with the *CSIS Act*.

1.4 Subsequent chapters of this policy will detail the specific policy and procedures to be followed when disclosing information and intelligence to the different clients of the Service.

1.5 The particular procedures for the disclosure, recording and tracking of information or intelligence collected pursuant to s. 16 of the *CSIS Act* are contained in OPS-222, "HUMINT Collection - Section 16" policy.

Authorities and References

1.6 *CSIS Act*

1.7 Ministerial Direction on CSIS Operations (2001 03 01)

1.8 Memorandum of Understanding between CSIS and the RCMP

1.9 Privy Council Office Directive of October 14 1986 on the Reporting of Security Investigations on Holders of Public Office

1.10 CSIS Operations Policies and Procedures

Definitions

1.11 See OPS-601, Appendix 1.

2. EXCEPTIONS

2.1 This policy **does not** regulate disclosures made:

i) to the Inspector General (IG) and the Security Intelligence Review Committee (SIRC) pursuant to their duties and functions;

ii) to the Secretariat of the Ministry of the Department of Public Safety and Emergency Preparedness Canada pursuant to the Minister's responsibilities under the *Act*;

iii) in response to requests made under the *Access to Information Act* and the *Privacy Act*;

iv) to other Canadian Government institutions for the purposes of the Service's administrative requirements, e.g. Treasury Board, Auditor General, National Archives.

3. PRINCIPLES

Legal requirements and Service policy

3.1 All Service disclosures of information obtained in the performance of its duties and functions must be authorized by in accordance with s. 19(2) or 19(2)(a) to (d) of the *CSIS Act*.

Protection of source and employee identity

3.2 Section 18(1) of the *CSIS Act* prohibits employees from disclosing any information from which can be inferred the identity of a past or present confidential source of information or assistance to the Service, or the identity of any past or present employee engaged in covert operational activities of the Service.

3.2.1 Such information may be disclosed in accordance with the conditions of s. 18(2) and after consultation with the Director General, Human Sources and Ops Support (DG HSOS) and with the approval of the Deputy Director, Operations (DDO).

Assessment

3.3 When making disclosures, employees must take into consideration the potential threat to the security of Canada, the national interests, the privacy of the person(s) and organization(s) concerned and operational necessity.

3.3.1 Employees must also assess the impact of disclosure on:

i) the safety of individuals;

ii) human and technical sources;

iii) investigative and collection techniques;

iv) the third party rule;

v) the possibility of disclosure through access to information legislation.

Discretion

3.4 In the course of operational activities, employees must exercise discretion and only disclose that information necessary to meet the Service's operational requirements.

4. RESPONSIBILITIES

Director

4.1 The Director is responsible for the reporting of security intelligence investigations involving holders of public office and for making disclosures in the public interest approved by the Minister pursuant to s. 19(2)(d) of the *CSIS Act*.

Director's Secretariat

4.2 The Committees and Ministerial Liaison Unit of the Director's Secretariat are responsible for the coordination of liaison between the Service and the Department.

HQ Directors General

4.3 HQ Directors General are responsible for:

i) requesting Ministerial approval for disclosures which must be authorized by the Minister;

ii) authorizing the regions to make certain disclosures and advising the regions on disclosure matters;

iii) authorizing the RCMP, in accordance with the CSIS-RCMP Memorandum of Understanding (MOU), to use Service information or intelligence in judicial proceedings;

iv) making disclosures to foreign agencies, institutions of the Government of Canada.

Regional Directors General

4.4 Regional Directors General, are responsible for disclosures to:

i) the RCMP regarding security offenses under the CSIS-RCMP MOU;

ii) local law enforcement agencies pursuant to s. 19(2)(a) of the *CSIS Act*;

iii) provincial government institutions.

4.4.1 Subject to other provisions of this policy, paragraphs 4.3 and 4.4 are not mutually exclusive, as responsibilities for some disclosures may be shared by both HQ and Regions.

NOTE: Conditions of disclosure conferred on Regional Directors General are located in OPS-602, "Disclosure of Security Information or Intelligence," section 3.

Intelligence Assessments Branch

4.5 The Director General, Intelligence Assessments Branch (DG IAB) has the primary responsibility for:

i) disclosing of information pursuant to s. 19(2)(b) and (c) of the *CSIS Act*; and
ii) coordinating the Service's response to Government institutions requesting assistance in preparing their threat or risk assessments.

Communications Branch

4.6 Communications Branch is responsible for answering public and media enquiries regarding

specific operational activities of the Service, after consultation with the HQ operational branches.

5. GENERAL POLICY

Arrangements

5.1 Disclosures by the Service must comply with the conditions of arrangements or MOU entered with institutions of the Government of Canada, provincial agencies and governments, and foreign agencies.

5.1.1 When applicable, the persons authorized in these arrangements or MOUs will make the disclosures on behalf of the Service.

Requests

5.2 Requests from domestic or foreign agencies for information or intelligence must be justified under the Service's mandate.

5.2.1 If it appears the request cannot be justified under the mandate, the matter will be brought to the attention of the Assistant Director, Operations (ADO) who will:

i) seek additional information from the requesting agency, or

ii) advise that the Service is not authorized to provide the requested information or intelligence.

Caveats

5.3 In order to control the subsequent use of information or intelligence disclosed by the Service, written disclosures to domestic or foreign agencies must be accompanied by appropriate caveats (OPS-603).

5.3.1 The Service may authorize, **in writing**, the original recipient(s) to further disclose Service information or intelligence to other parties.

Verbal disclosures

5.4 When making verbal disclosures, employees must sensitize the recipients to the confidentiality of the information or intelligence disclosed, and on the need to limit further dissemination.

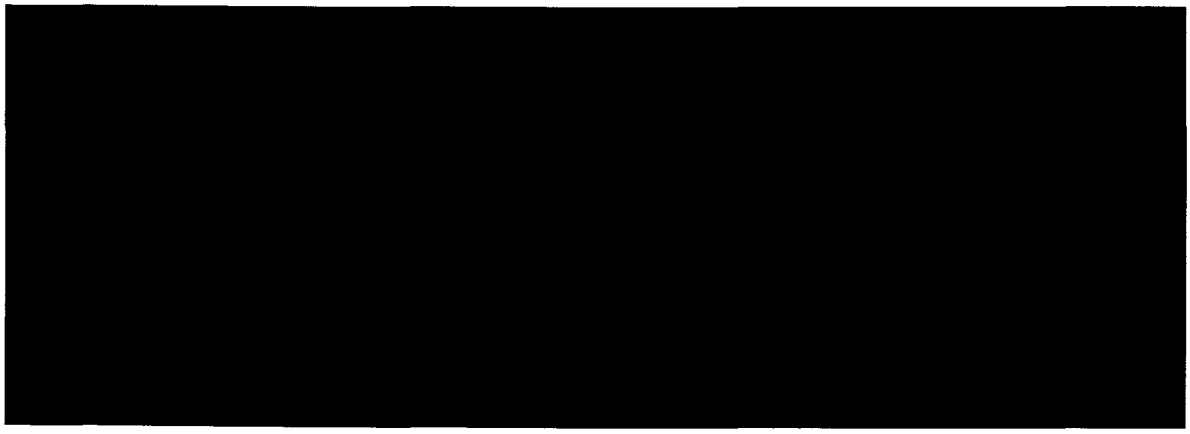
5.4.1 Employees must record verbal disclosures in the appropriate file.

Reporting

5.5 For reasons of accountability and security, reports of disclosures must be placed on the appropriate operational file and contain such details as the identity of the recipient, circumstances of disclosure and the nature and extent of the information or intelligence disclosed.

5.5.1 Operational sectors must maintain a record of information or intelligence exchanged with domestic or foreign agencies.

NOTE: Refer to Information Management Branch (IM) procedures for the recording of disclosed s. 12 information in the BRS database.



From: [redacted]
To:

Date: 2005-06-06 11:37:16 AM
Subject: MEETING WITH NATIONAL ENERGY BOARD

iClassification: Secret
Classification: Secret

[redacted]

Further to various correspondance regarding a request for assistance by the National Energy Board (NEB) located in Calgary, the following is a summary of discussions with the NEB locally.

On 2005 05 16 I met with Leo Jansen and Jamie Kereluk (both of Operations Compliance) at the NEB office in Calgary. For the uninitiated, the NEB is an federal agency headquartered in Calgary (as opposed to Ottawa) which regulates the pipeline industry and energy development in Canada. They are responsible for compliance (and as of recently, security) issues when pipelines cross provincial or national boundaries, for hydroelectic issues when they cross international borders, etc. The purpose of our meeting was to discuss the roles and tasks of both the NEB and the Service (they were unfamiliar with details of our role) and establish contact locally. Both Jansen and Kereluk hold level II clearances.

The NEB, as a federal agency, is independent, but answers to Parliament through the Minister of Natural Resources (NRCan). Given that they are located in Calgary, the NEB often feel 'left out' of discussions with federal partners, yet feel a need to have some link into the federal security apparatus.

The NEB recently completed a study of critical infrastructure under their purview across Canada. They are now wondering what to do with the report given its classification (Confidential). I suggested they may wish to speak with PSEPC on the matter.

[redacted]

[redacted] for our purposes, the NEB advised that they currently receive only unclassified ITAC reports (via PSEPC in Edmonton), and these through a secure fax in their Calgary office. They do not receive applicable Laser reporting or classified ITAC reports, and currently do not have any electronic means of receiving them (save the fax). Jansen requested that the Service consider a way in which Laser reporting could be provided to them and advised that they have secure facilities to store up to TS (I am not aware who completed the certification).

As the NEB is a federal agency with a specific security mandate, it is logical that they should be included in Laser dissemination when the reporting refers to threats to the energy sector. Given the potential difficulty of transmitting classified documents to them electronically at this time, Calgary District will undertake to provide hard copies locally if so directed by PR and HQ.

Cheers,

[redacted]

PS: Pardon the delay in filing this note as we were awaiting assignment of a file number. [redacted]

[redacted]

cc: [redacted]

2001-11-28
OPS-602 DISCLOSURE OF SECURITY INFORMATION OR INTELLIGENCE

1. INTRODUCTION

Scope

1.1 This policy outlines the different circumstances under which information or intelligence may be disclosed and prescribes the policy and procedures to be followed when doing so.

2. DISCLOSURE OF INFORMATION TO THE CANADIAN GOVERNMENT

Channels of Disclosure

2.1 The absence of a CSIS Act, section 17 arrangement with a federal institution does not preclude the Service from making disclosures to selected officials of the institution.

2.2 The Service may make disclosures through participation in interdepartmental committees.

2.3 The Service shall disclose relevant information and provide advice to other Government institutions requesting assistance in preparing their threat or risk assessments.

2.3.1 The Research, Analysis and Production Branch shall coordinate the Service's response to those Government institutions through consultations with other operational branches, and maintain a record of all institutions requesting advice on risk assessments.

Parliament Security Services

2.4 The Service shall disclose to the RCMP all threat information relevant to the Security Services of the House of Commons and the Senate Protective Service.

2.4.1 The Director must approve the disclosure of unique or special information directly to the Parliamentary Security Services.

Screening

2.5 Disclosures for purposes falling under sections 13 and 14 of the CSIS Act are governed by the Government Security Screening Policy (OPS-108) and Service policies dealing with immigration and citizenship security screening.

Holders of Public Office

2.6 Disclosures relating to investigation(s) of holders of public office are to be made in accordance with the following guidelines from the Privy Council Office.

NOTE: See OPS-201, "Conduct of Operations - General" and "OPS-202, "Conduct of Operations - Fundamental Institutions of Society" for policy pertaining to senior public officials.

2.6.1 The reporting of any information or intelligence collected pursuant to section 12 of the CSIS Act concerning holders of public office shall be at the discretion of the Director.
2.6.2 The Director shall report to the Prime Minister, through the Secretary to the Cabinet, information or

intelligence regarding security intelligence investigations involving persons appointed to public office on the Prime Minister's recommendation.

2.6.3 In cases where the Prime Minister has no direct interest, the Director shall report on those holders of public office to the Minister of Public Safety and Emergency Preparedness.

2.6.4 In the case of judicial appointments, other than those identified in paragraph 2.6.5, the Director shall report to the Minister.

2.6.5 The list of holders of public office appointed on the Prime Minister's recommendations consists of:

i) Cabinet Ministers;

ii) Parliamentary Secretaries;

iii) Chief Justices of Superior Courts;

iv) Deputy Ministers; and,

v) Heads of agencies and Crown corporations.

2.6.6 All information concerning security intelligence investigations of holders of public offices shall promptly be reported to the relevant Headquarters branch, which will assess the information and prepare a report for the Director.

3. DISCLOSURE OF INFORMATION TO PROVINCIAL GOVERNMENTS AND AGENCIES

Conditions

3.1 The Service shall only make disclosures to Canadian provincial governments and agencies under one of the following conditions:

3.1.1 Pursuant to the general authority contained in the preamble of subsection 19(2) of the CSIS Act; disclosures made under this condition must benefit the Service in the performance of its duties and functions.

3.1.2 Pursuant to paragraph 19(2)(a) of the CSIS Act.

3.1.3 When the Minister authorizes the Service to disclose information as his/her agent. (See paragraph 10).

Consultation and Reporting

3.2 Prior to disclosing information to a provincial government or agency pursuant to paragraphs 3.1.1 and 3.1.3 above, the Region will consult with the relevant HQ branch.

3.2.1 The Region will report any disclosure to a provincial government or agency as per OPS-601, paragraphs 5.4 to 5.5.1.

Warning

3.3 Provincial access to information legislation has been developed which may affect the ability of departments/agencies to protect CSIS information disclosed to them under the auspices of this policy.

Security assessments

3.4 The Service may disclose security assessment information to provincial government and agencies when permitted by an arrangement pursuant to paragraph 13(2)(a) of the CSIS Act.

4. DISCLOSURE OF INFORMATION TO FOREIGN AGENCIES

Arrangement

4.1 In the absence of a CSIS Act section 17 arrangement with a foreign agency, the Service shall only make disclosures with the approval of the Minister.

4.1.1 In the event the Minister is unavailable to approve a temporary arrangement facilitating the disclosure, the Director is authorized to undertake whatever exchanges or cooperation that are necessary to address the requirement. The Director will advise the Deputy Minister of his decision and seek the Minister's approval as soon as possible thereafter.

4.1.2 In order to assess potential advantages to the security of Canada, Service employees may, on a case-by-case basis and with the approval of the Director, have contact with representatives of foreign agencies having no arrangement with the Service.

4.1.3 Such contacts shall involve only the disclosure of information of a general nature on the Service's role and interests.

Evaluation

4.2 Prior to making any disclosure to a foreign agency, employees shall consider:

i) the extent of the authorized agreement between the Service and the agency;

ii) the potential use of the Service's information or intelligence, especially if it concerns Canadians;

iii) Canadian national interests; and

iv) the ability of the foreign agency to protect Service information from disclosure under their access to information laws.

4.2.1 If, following the evaluation, there is doubt regarding the propriety of making a disclosure to a foreign agency, the Deputy Director General of Operations of the relevant branch shall decide if the disclosure should be made.

Foreign Liaison Advisor

4.3 The Foreign Liaison Advisors within the operational branches shall assist and advise employees in evaluating the conditions of disclosure.

Evidence

4.4 The Service shall not disclose to a foreign law enforcement or security intelligence agency, any information or intelligence obtained in the performance of its duties and functions, if the foreign agency intends to use the information for evidentiary purposes, unless the Service:

i) consults with Legal Services on the matter; and,

ii) obtains the prior approval of the Deputy Director, Operations (DDO).

Unlawful activities

4.5 Information or intelligence obtained by the Service which relates to unlawful activities of a serious nature of interest to a foreign country shall be promptly reported to the relevant HQ branch.

4.5.1 This information may be disclosed, after consultation with Legal Services, to the relevant foreign authorities.

5. SELECTIVE DISCLOSURES

Public or private sector

5.1 The Service may, with proper care and caution, make disclosures to members of the public or the private sector, in order to carry out mandated investigations and programs. Employees may make the necessary disclosures on a strict need to know basis.

5.1.1 When making such disclosures, employees must exercise caution to ensure that:

i) the Service's sources and methodologies are protected to the fullest extent possible; and,

ii) the rights, privacy and employment of an individual are not unnecessarily placed at risk.

NOTE: See OPS-201, "Conduct of Operations - General" and OPS-202, "Conduct of Operations - Fundamental Institutions of Society".

6. DISCLOSURE OF INFORMATION RELATING TO THE SECURITY OFFENSES ACT

Jurisdiction

6.1 The RCMP has the primary responsibility to perform duties assigned to peace officers in relation to any offence in section 2 of the Security Offenses Act. "Threats to the security of Canada" defined in section 2 of the CSIS Act, constitute security offenses.

Discussions

6.1.1 When the Service and police forces other than the RCMP are holding discussions on matters likely to overlap the enforcement of security offenses, the RCMP should be informed or invited to attend the discussions.

6.1.2 This provision does not preclude routine liaison and exchange of information between the Service and police forces other than the RCMP.

Provision of Information and Intelligence

6.2 The Service will disclose to the RCMP, on a timely basis or upon specific request, information and intelligence relevant to RCMP responsibilities in relation to security offenses, in accordance with the Memorandum of Understanding between the RCMP and the Service.

6.2.1 The Counter Terrorism Branch has adopted specific procedures for disclosures to the RCMP (see OPS-602-1, "Procedures - Disclosure of Security Information or Intelligence to RCMP").

Liaison

6.3 The RCMP liaison officers posted in the Service's regional offices and HQ are granted access to Service information and intelligence to identify what may be of interest to the RCMP regarding their responsibilities in the enforcement of the Security Offenses Act.

6.3.1 Following identification, the RCMP liaison officer requests the disclosure of information or intelligence. Upon the Service concurrence, disclosures to the RCMP are made by using the formal disclosure channels agreed upon by the two agencies.

HQ or Region

6.4 A regional or HQ Director General (or designate) may authorize disclosures to the RCMP regarding security offenses.

Judicial proceedings

6.5 The provision of advisory letters to the RCMP allowing the RCMP to use Service information or intelligence in judicial proceedings (e.g. the obtaining of warrants, evidence in court) shall be approved by the relevant HQ Director General. (In some instances, a higher level of authority may be required, refer to paragraph 7 of the CSIS-RCMP MOU.)

Emergencies

6.6 In emergencies where immediate police action is required to prevent unlawful activity of a serious nature against persons or property, employees may promptly report to the police force with the primary jurisdiction and the RCMP shall be advised as soon as possible thereafter.

6.6.1 The regions shall immediately advise HQ after making such disclosures.

7. DISCLOSURE OF LAW ENFORCEMENT INFORMATION

Discretion

7.1 Paragraph 19(2)(a) of the CSIS Act, gives the Service discretion to disclose incidental information obtained in the performance of its duties and functions, if the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province.

7.1.1 This information may be disclosed to:

i) A peace officer having jurisdiction to investigate the alleged contravention; and,

ii) The Attorney General of Canada and the Attorney General of the province in which the

proceedings in respect of the alleged contravention may be taken.

Authority

7.2 The relevant HQ or regional Director General may authorize disclosures of law enforcement information; the DG may designate employees who will be responsible for making such disclosures.

7.3 Regions shall advise Headquarters in a timely fashion of disclosures to local law enforcement agencies.

7.4 Employees shall weigh the seriousness and consequences of the alleged contravention against the impact of the disclosure on the Service's operations.

Serious unlawful activities

7.5 When there are reasonable grounds to suspect unlawful activities of a serious nature, the Service may report these suspicions to a peace officer having primary jurisdiction to investigate the alleged contravention.

7.5.1 Should the Service determine that the disclosure of such information would be detrimental because of operational or national interests, it shall immediately refer the matter to the Minister.

State of information

7.6 The Service should not comment upon or analyse information for the benefit of law enforcement agencies, beyond what is required for comprehension. However, the Service may comment on the reliability of the source of information without revealing the source's identity.

7.7 Procedures as detailed in OPS-602-2 are to be followed when disclosing law enforcement related information to peace officers other than the RCMP.

8. DISCLOSURE OF INFORMATION UNDER 19(2) (b) AND (c) OF THE CSIS ACT

Discretion

8.1 The CSIS Act provides the Service the discretion to disclose incidental information obtained in the performance of its duties and functions, if this information relates to the conduct of the international affairs of Canada or to the defence of Canada.

Foreign Affairs or National Defence

8.2 Disclosures under paragraph 8.1 may accordingly be made to:

i) the Secretary of State for Foreign Affairs or the Minister of National Defence; or,

ii) persons designated for this purpose by the responsible Minister.

Research, Analysis and Production Branch

8.3 Pertinent incidental information shall promptly be forwarded to the Research, Analysis and Production Branch (RAP) with appropriate comments, source assessment and recommendations.

8.3.1 RAP will coordinate the disclosure of the information to Foreign Affairs and National Defence. If necessary, RAP will consult with the appropriate operational branch before disclosing the information.

8.3.2 The DG RAP or designate may authorize disclosures of paragraphs 19(2)(b) and (c) of the CSIS Act spin-off information.

State of information

8.4 RAP may comment on or analyse incidental information for the benefit of the recipient department and comment on the reliability of the source of information and should avoid, when possible, revealing the source's identity.

9. DISCLOSURE OF INFORMATION IN THE PUBLIC INTEREST

Discretion

9.1 Paragraph 19(2)(d) of the CSIS Act gives the Service the discretion to disclose incidental information obtained in the performance of its duties and functions if, in the opinion of the Minister, the disclosure is essential in the public interest and that interest clearly outweighs any invasion of privacy that could result from the disclosure.

9.1.1 The Minister may authorize the Service to disclose the information to:

i) any minister of the Crown;

ii) a person in the public service of Canada.

Director

9.2 The relevant HQ branch shall promptly forward through the Assistant Director, Operations (ADO) to the Deputy Director, Operations with appropriate comments and source assessment, information which may be disclosed in the public interest. The HQ Branch shall also advise the Ministerial Liaison Unit of the Secretariat who will coordinate correspondence with the Department of Public Safety and Emergency Preparedness.

9.2.1 The Director is responsible for making the disclosures to the authorized recipients.

Report to SIRC

9.3 The Director shall, as soon as practicable, submit a report to the Security Intelligence Review Committee (SIRC) regarding disclosures made in the public interest.

10. SPECIAL DISCLOSURES
Minister's agent

10.1 The Service shall only make disclosures outside the Government of Canada in accordance with this policy. In instances where the Service believes that the national interest warrants the disclosure of security information or intelligence outside the Government of Canada, the Service may recommend to the Minister that such information be disclosed by him/her.

10.1.1 If the Minister does not exercise this discretion, he/she may authorize the Service acting as his/her agent, to make the disclosure to:

i) Members of Parliament and Senators who are not Ministers of the Crown;

ii) governments, elected officials and institutions of the provinces and municipalities;

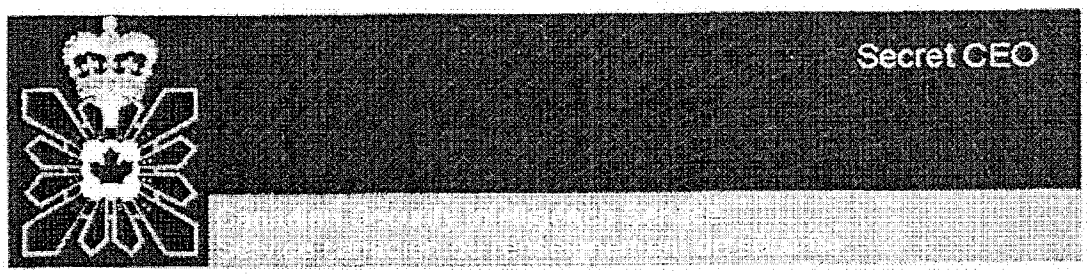
iii) the private sector.

Report to SIRC

10.2 The Director shall, as soon as practicable, submit a report to the Security Intelligence Review Committee (SIRC) regarding disclosures made in the national interest.

TAB

1



Intelligence Requirements 2011 / 2012

2011/12 Intelligence Requirements

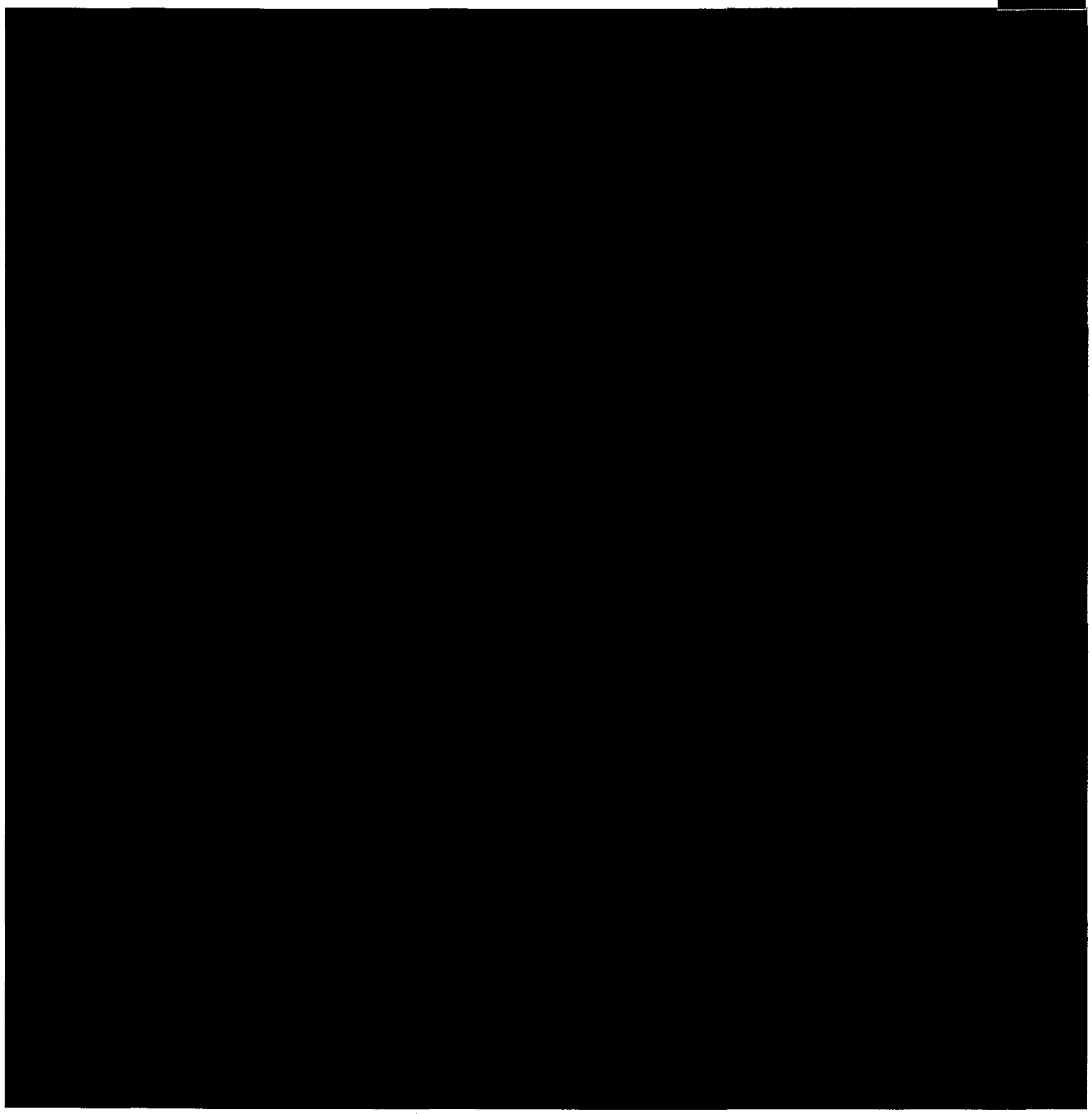
INTELLIGENCE REQUIREMENTS 2011/2012 - PROCEDURES

The following Intelligence Requirements Documents (IRDs) have been prepared by IAB in consultation with CSIS operational branches. They reflect both Service and Government of Canada (GoC) intelligence requirements and are intended to guide CSIS collection and reporting.

Intelligence Requirements (IRs) are not collection authorities. They represent a collation of requirements and interests that will enable CSIS to effectively advise the GoC about threats to Canada and Canadians, and to meet Canada's broader foreign policy, trade, and commercial interests. Any collection against these requirements must be done in accordance with the appropriate Section 12 targeting authority, or under Section 16 where ministerial approval has been granted.

[redacted]

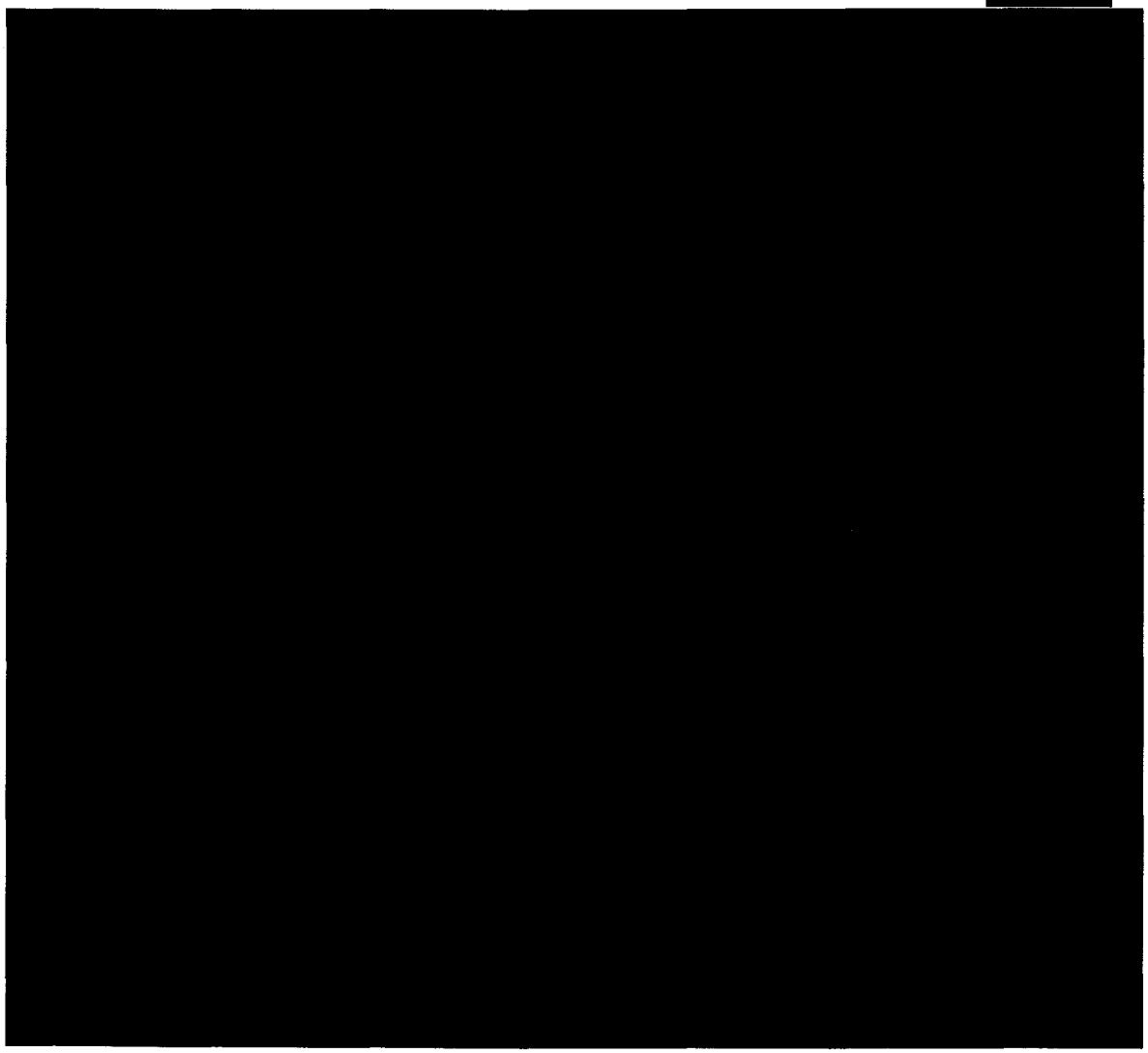
2



[redacted]

DOMESTIC EXTREMISM INTELLIGENCE REQUIREMENTS (IRs)

[redacted]



TAB

2

Intelligence Assessment

SECRET / CANADIAN EYES ONLY [redacted]

2012 03 23

2012 Domestic Threat Environment In Canada [redacted]

Summary

[redacted]

[redacted]

[redacted]

CAVEAT

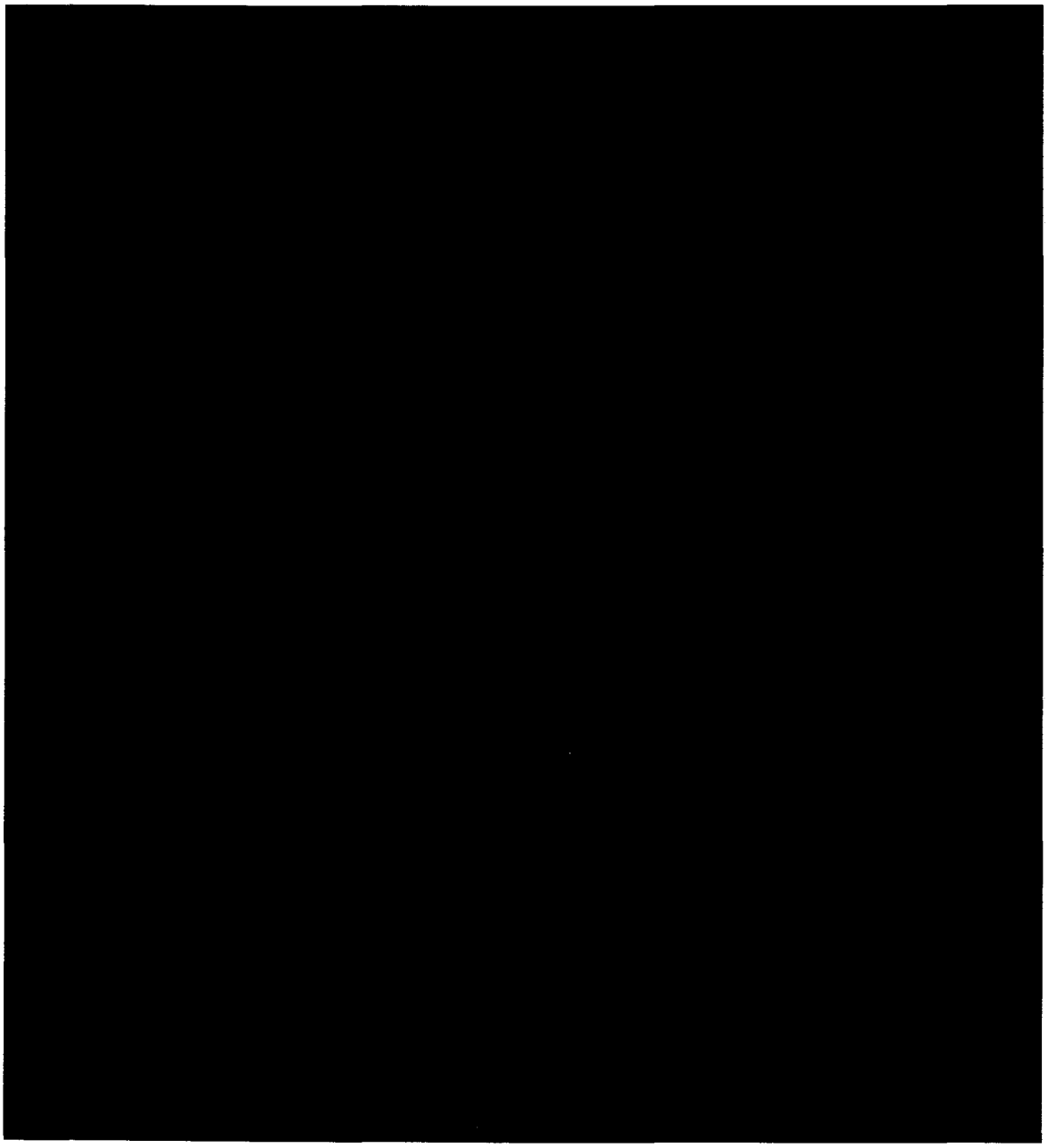
This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency/department in confidence. The document must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

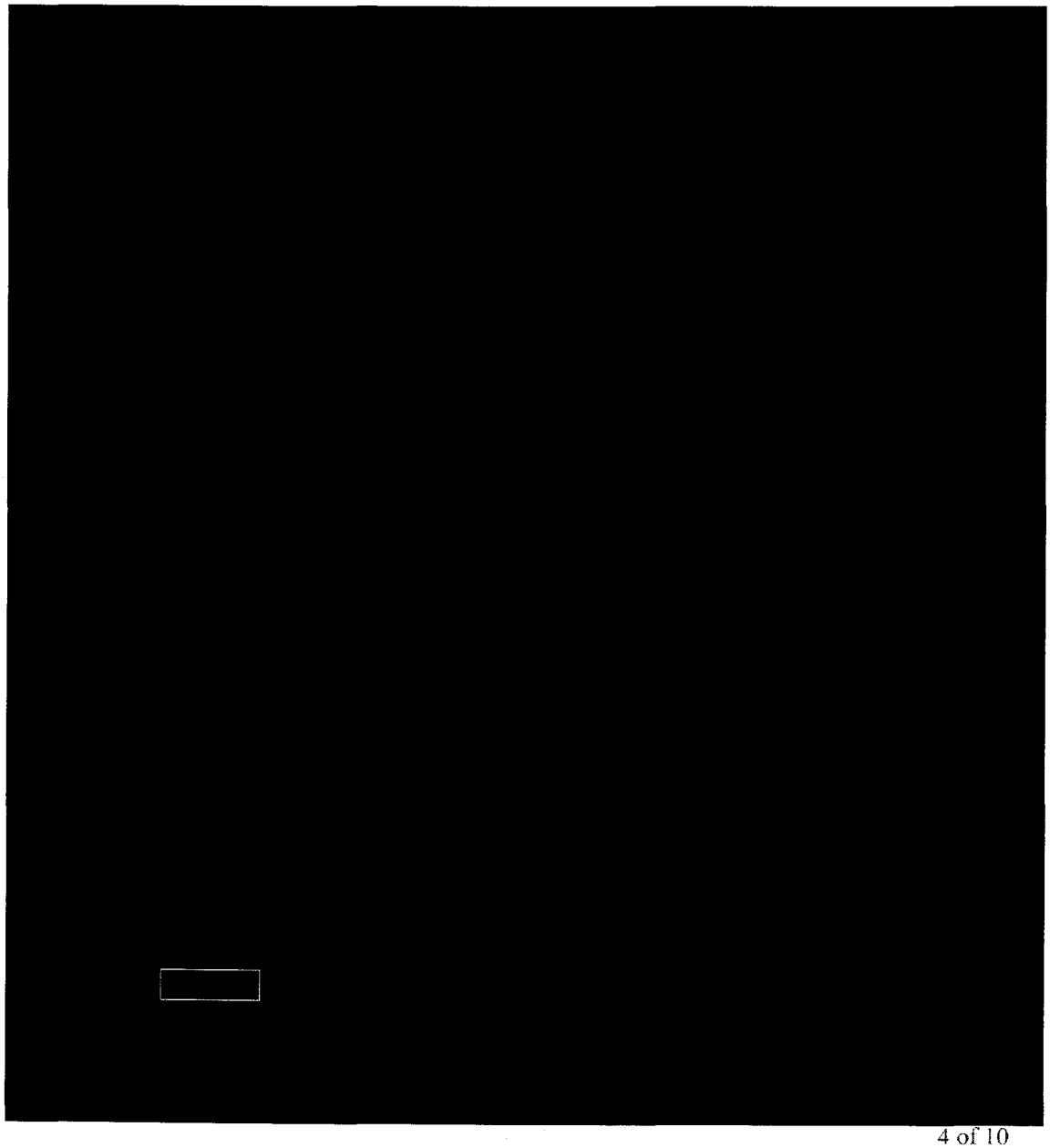
Canadian departments, agencies or organizations: This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

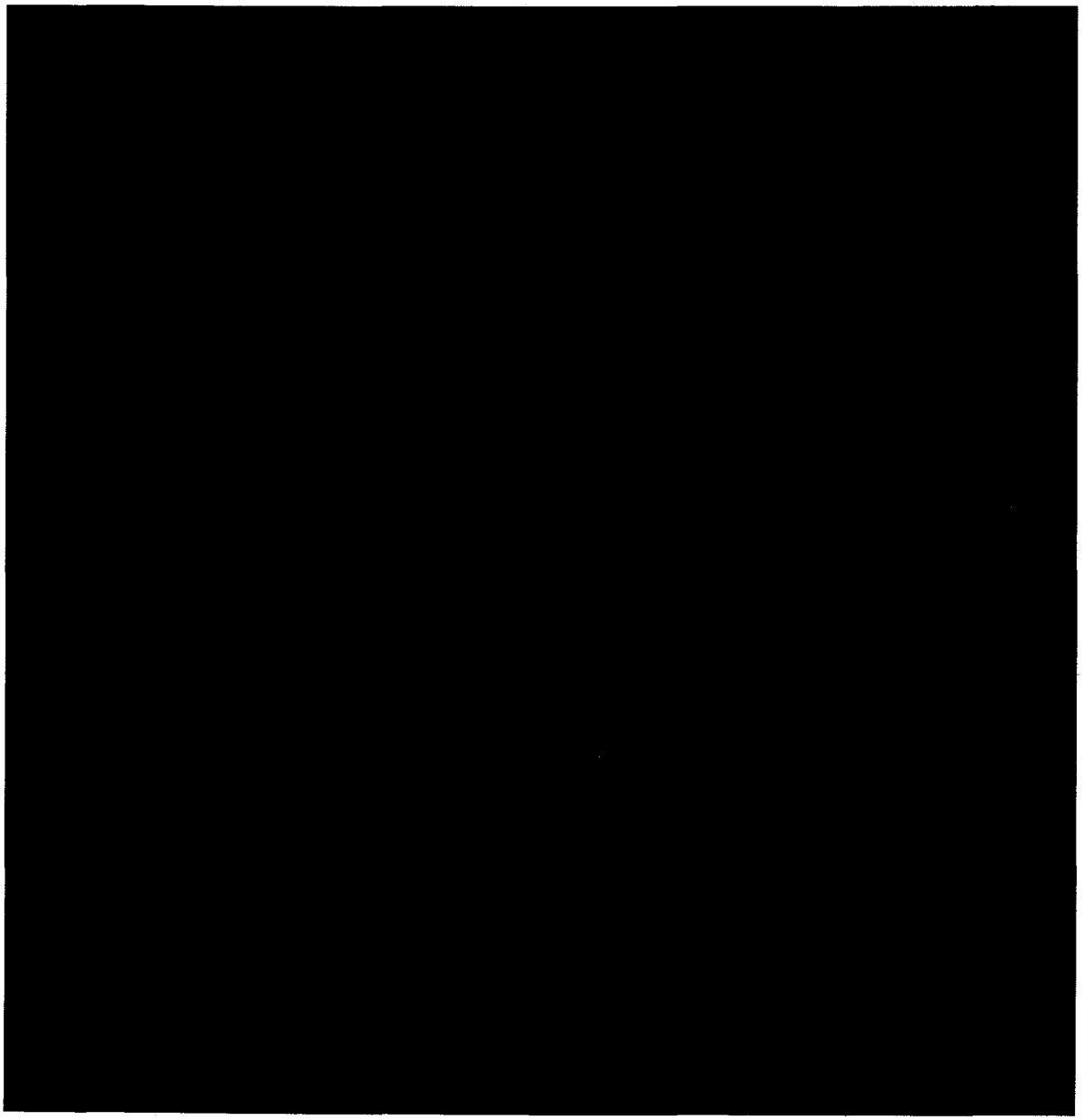
Foreign agencies or organizations: This document is loaned to your agency/department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

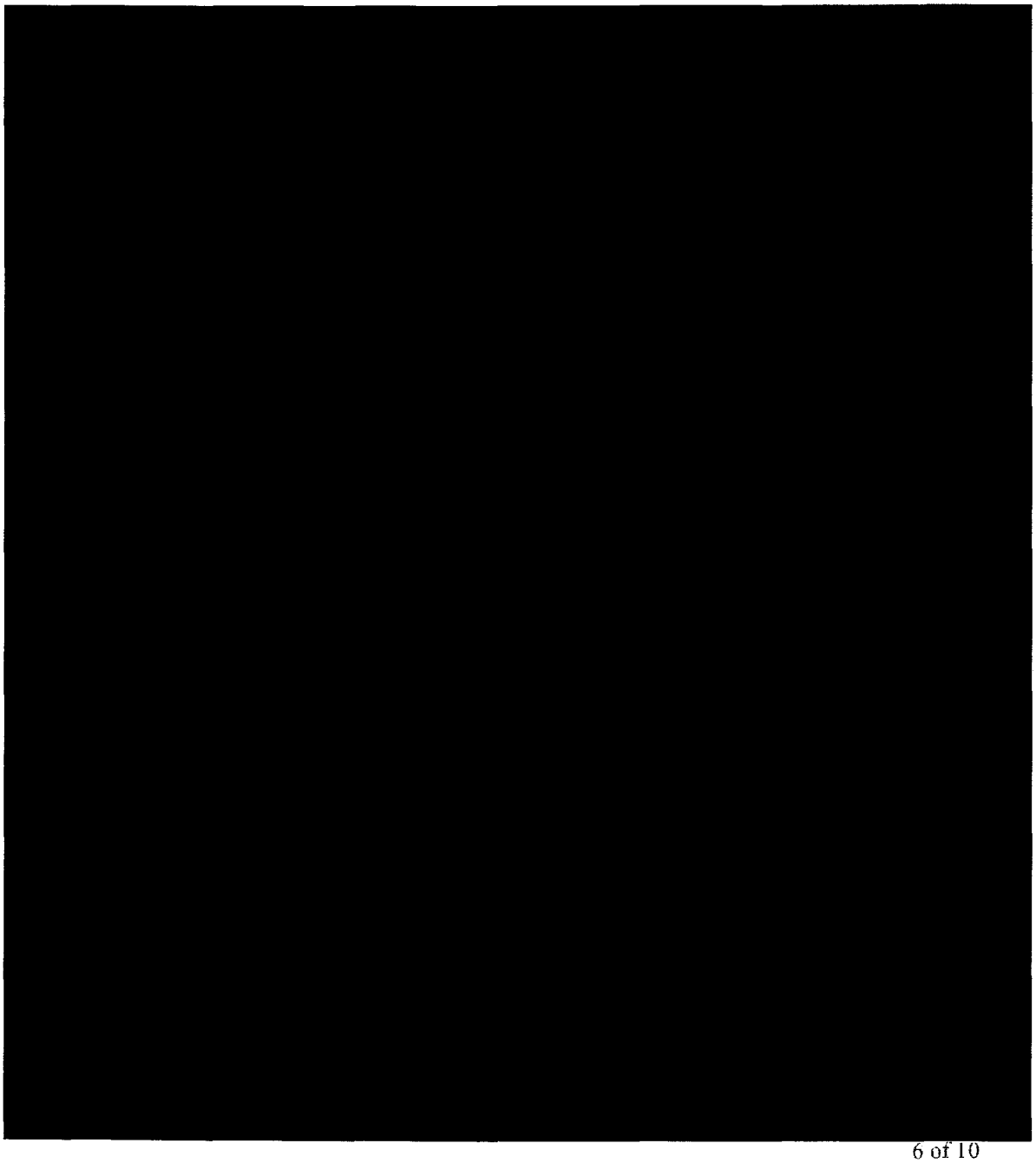
Introduction

[redacted]

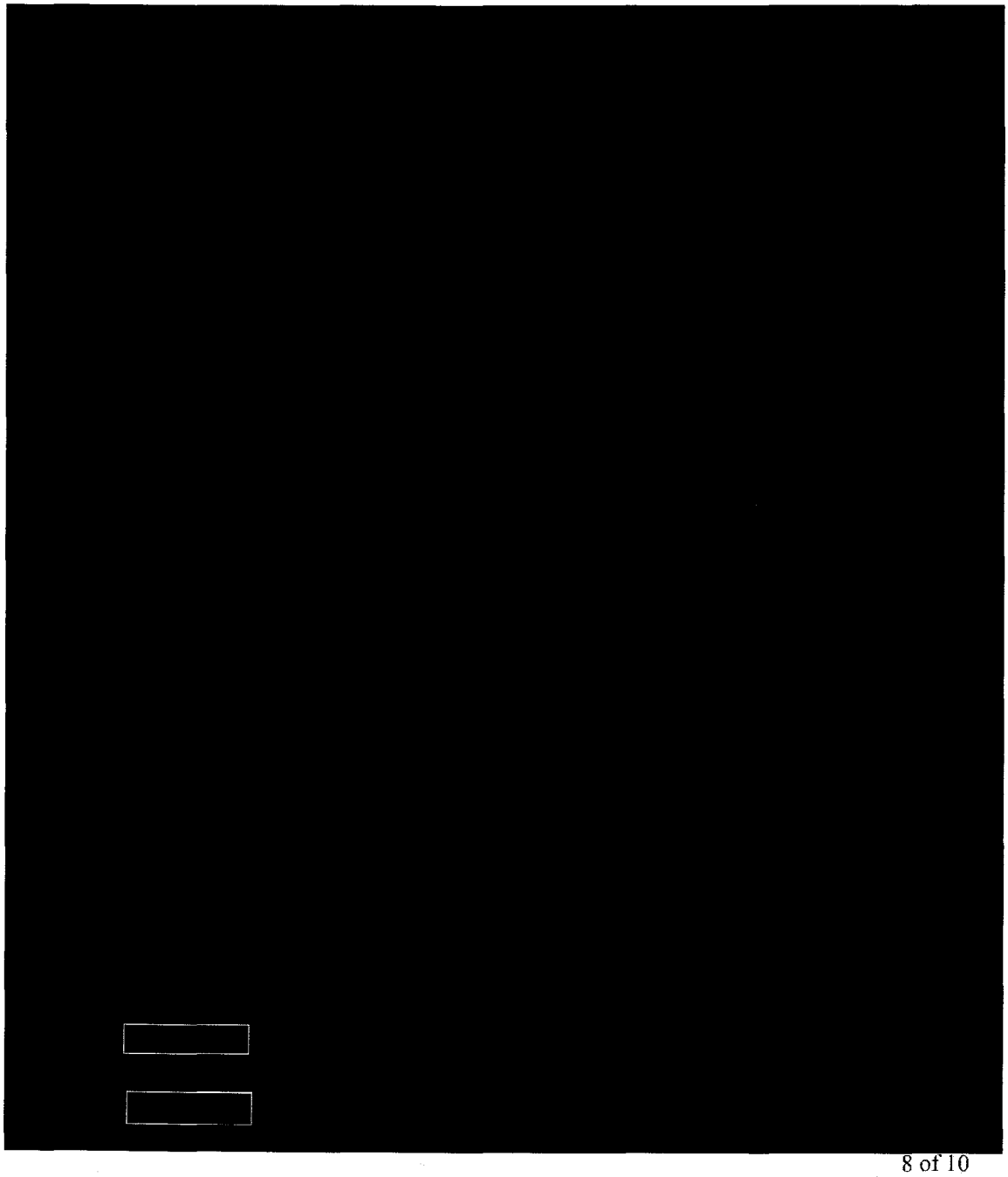


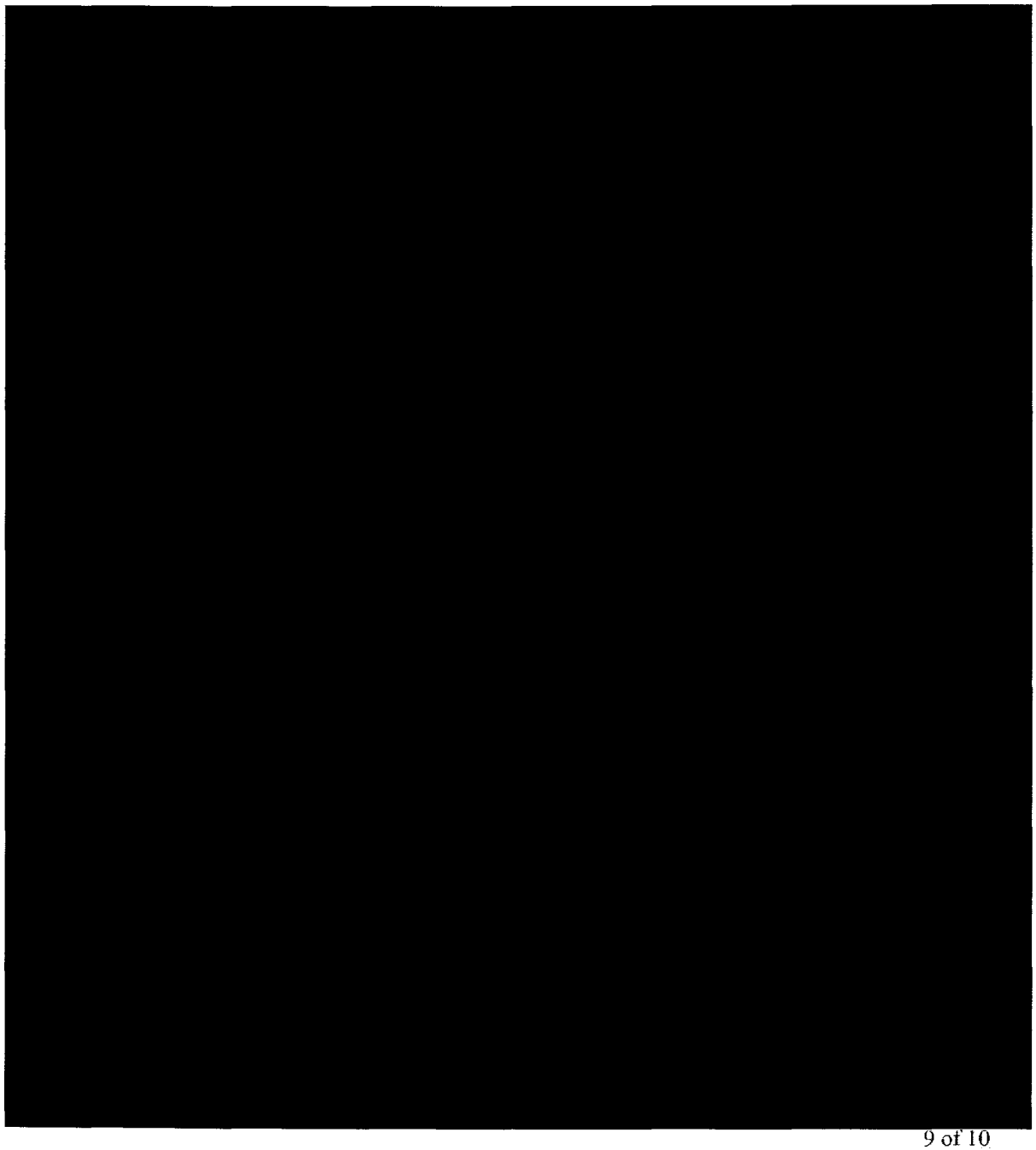






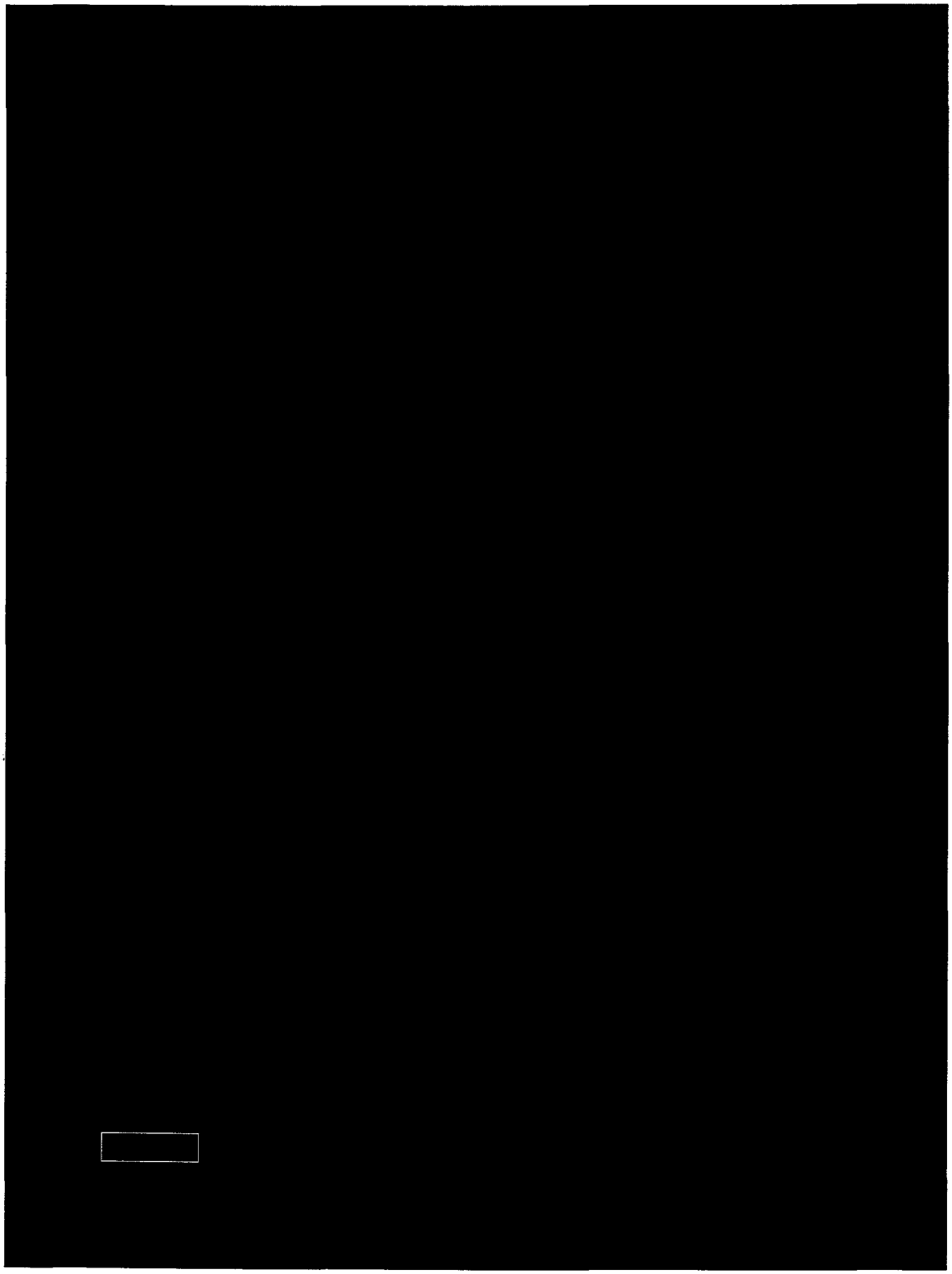
[redacted]

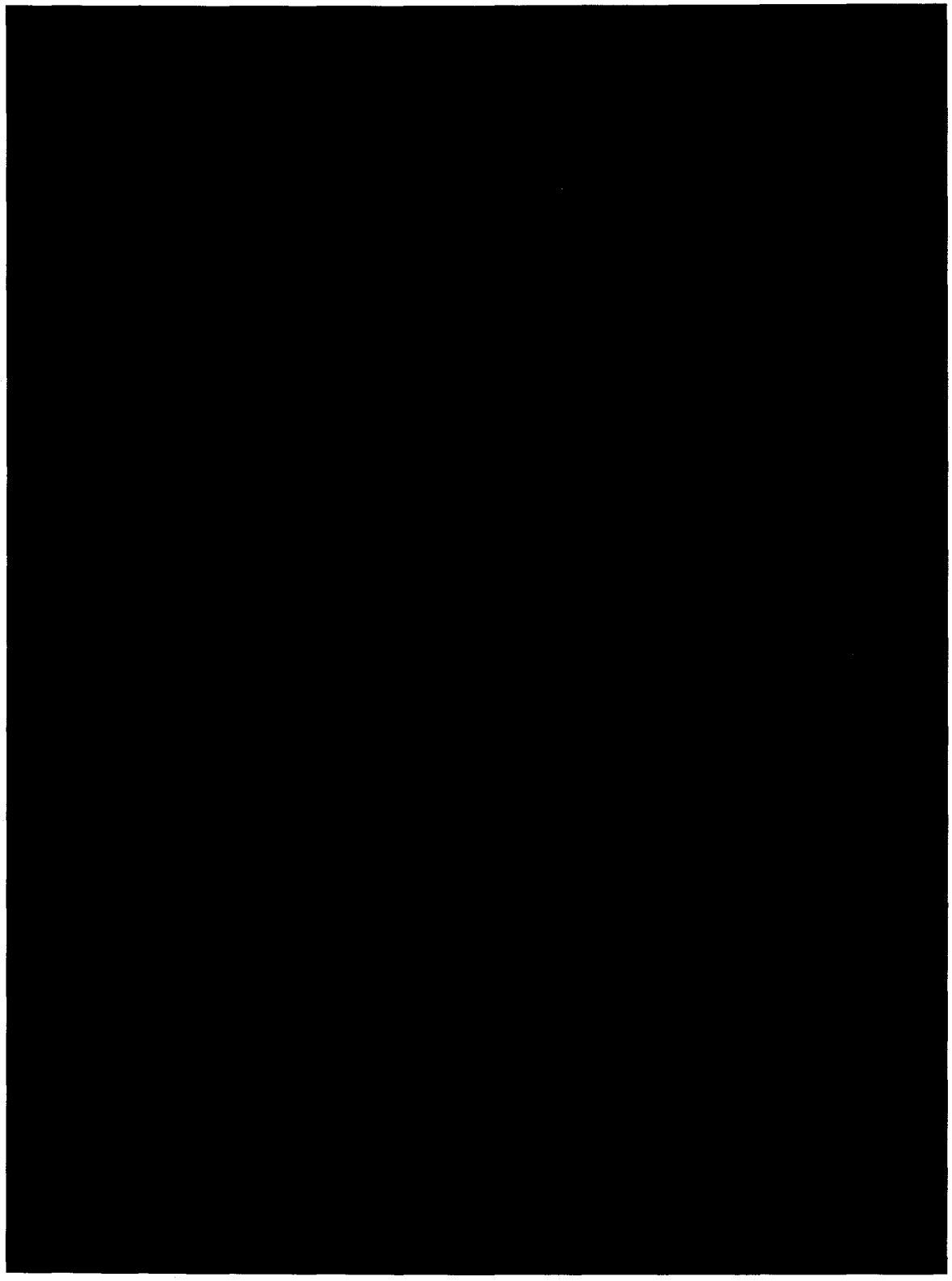




[redacted]

[redacted]

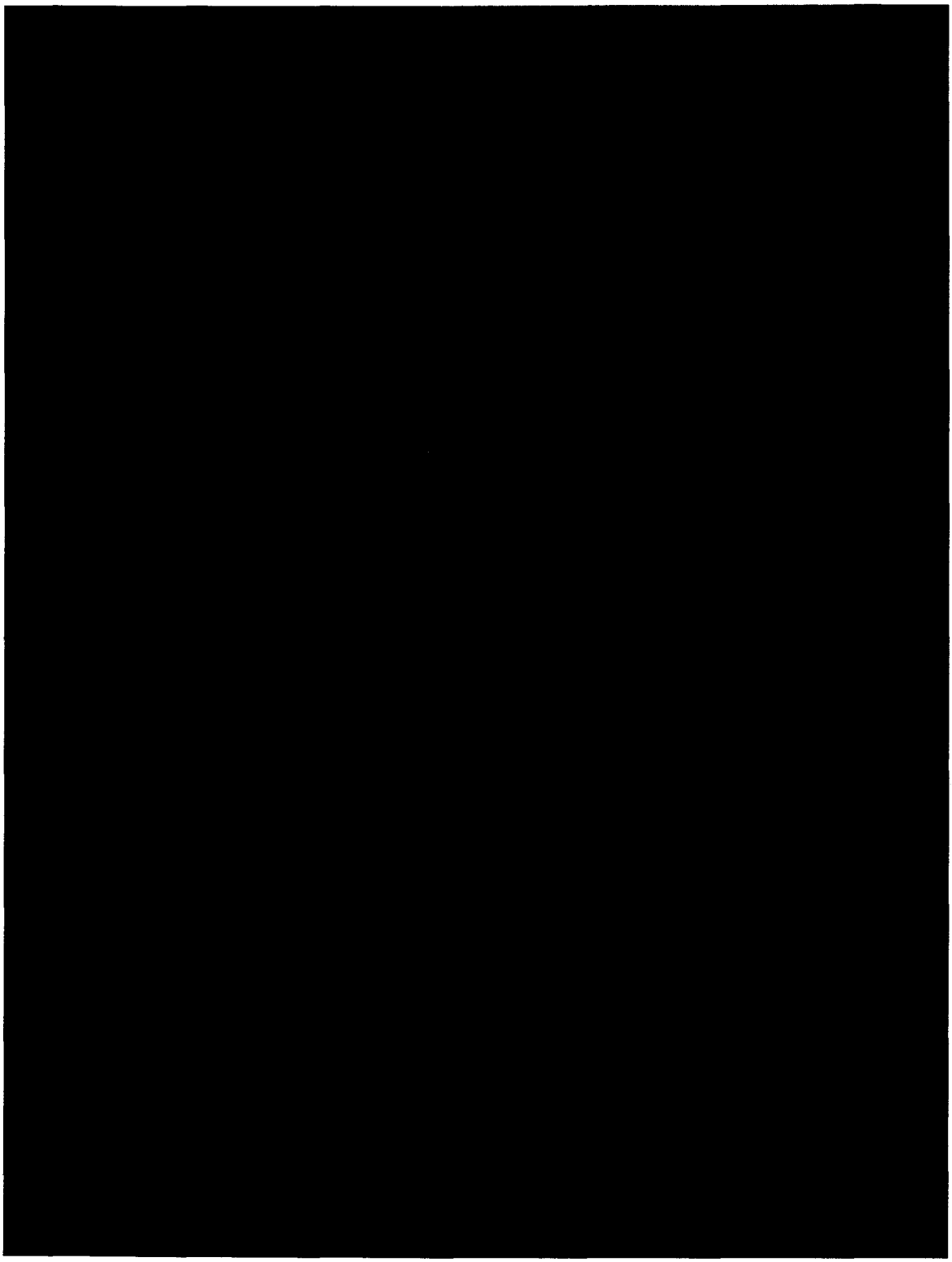


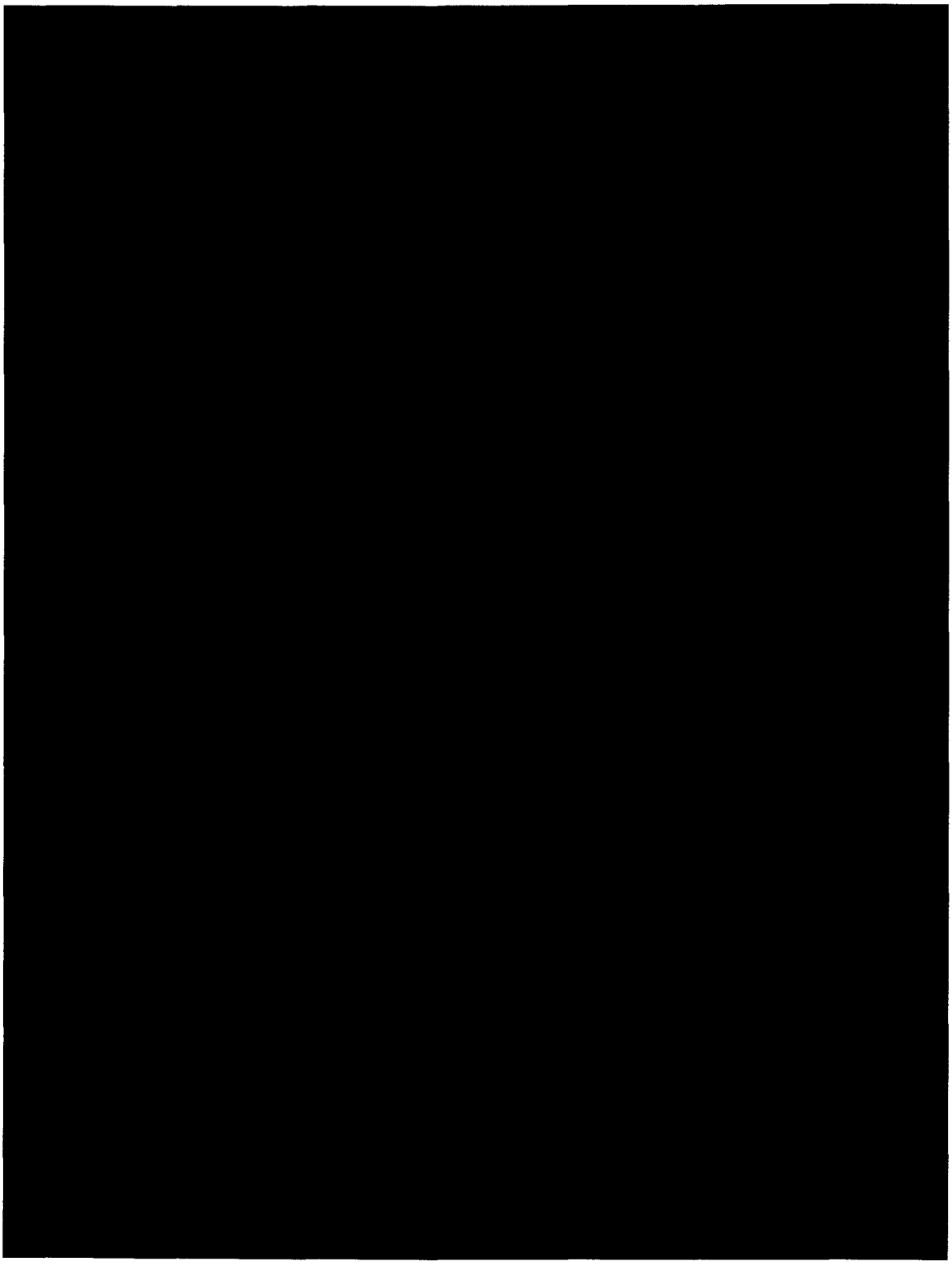


[redacted]

[redacted]

[redacted]





[redacted]

HEAD, IAB – TERRORISM / EXTREMISM
[redacted]

[redacted]

[redacted]

2013 01 23

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

For information on Topics Related to this Intelligence Assessment
Please see the Following Service Products:

[redacted]

[redacted]

CAVEAT

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency/department in confidence. The document must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Canadian departments, agencies or organizations: This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

Foreign agencies or organizations: This document is loaned to your agency/department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

CSIS SCRS

Intelligence Assessment
Évaluation du renseignement

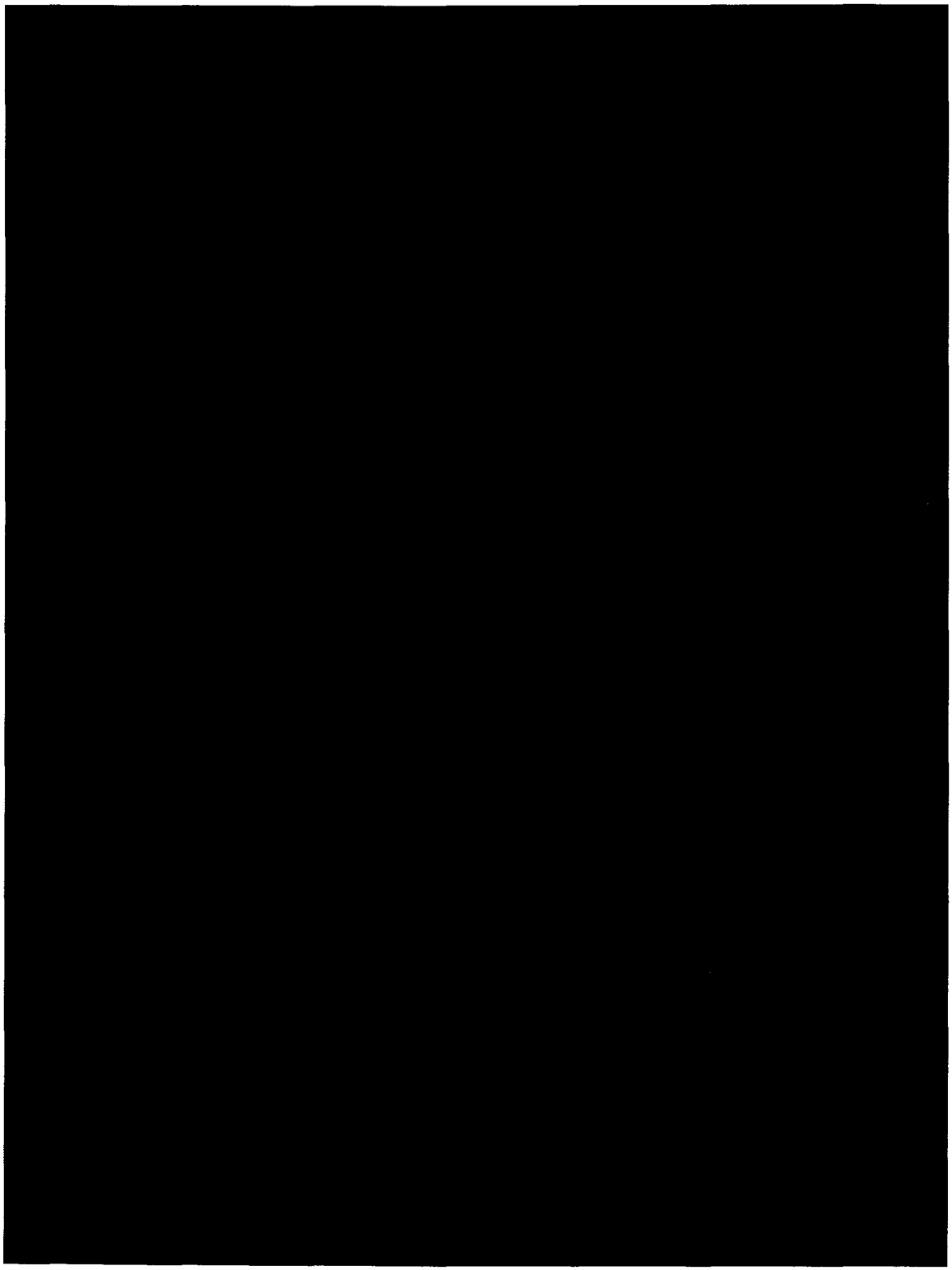
SECRET//CEO

[redacted]

2015 01 19

[redacted]

[redacted]



[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

CAVEAT

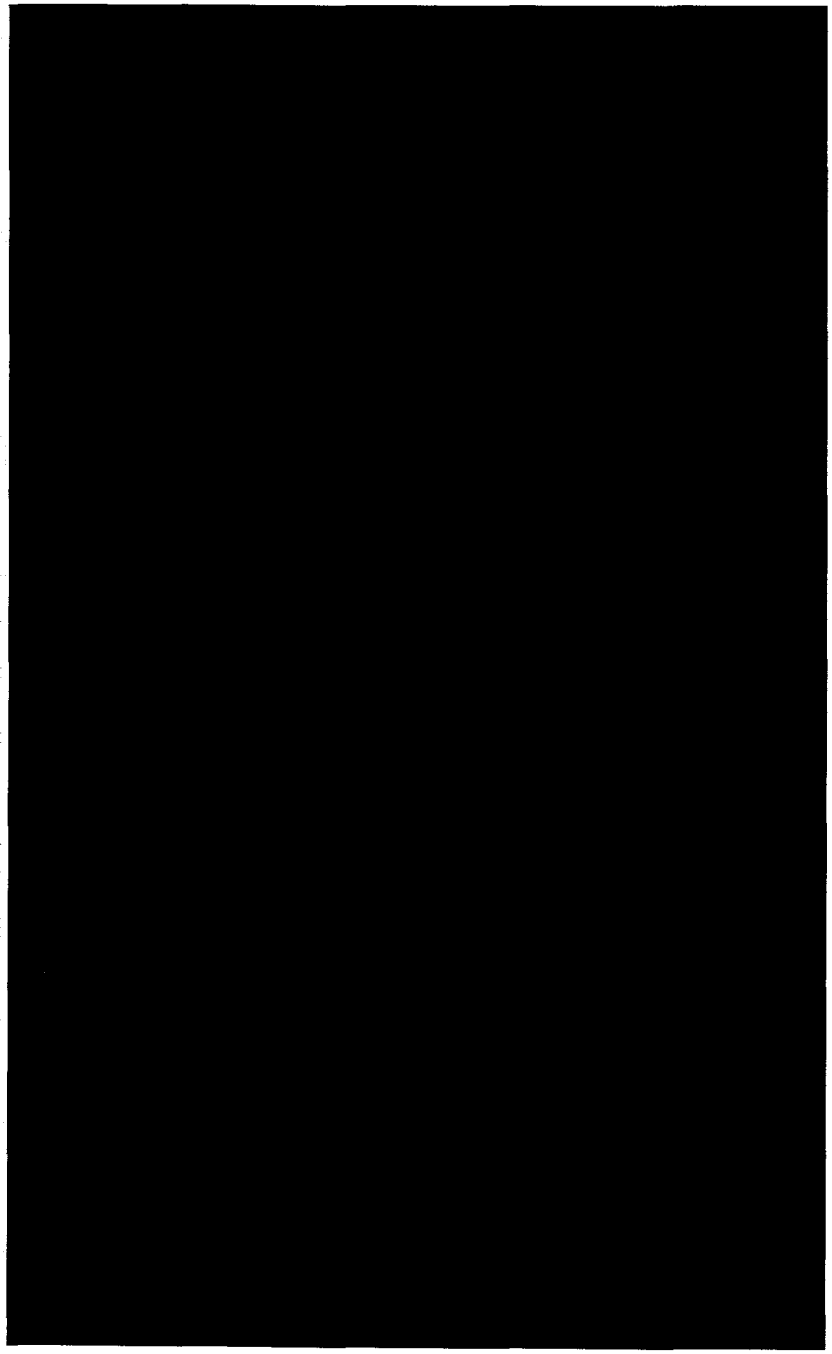
This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency/department in confidence. The document must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Canadian departments, agencies or organizations: This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

Foreign agencies or organizations: This document is loaned to your agency/department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

TAB

3

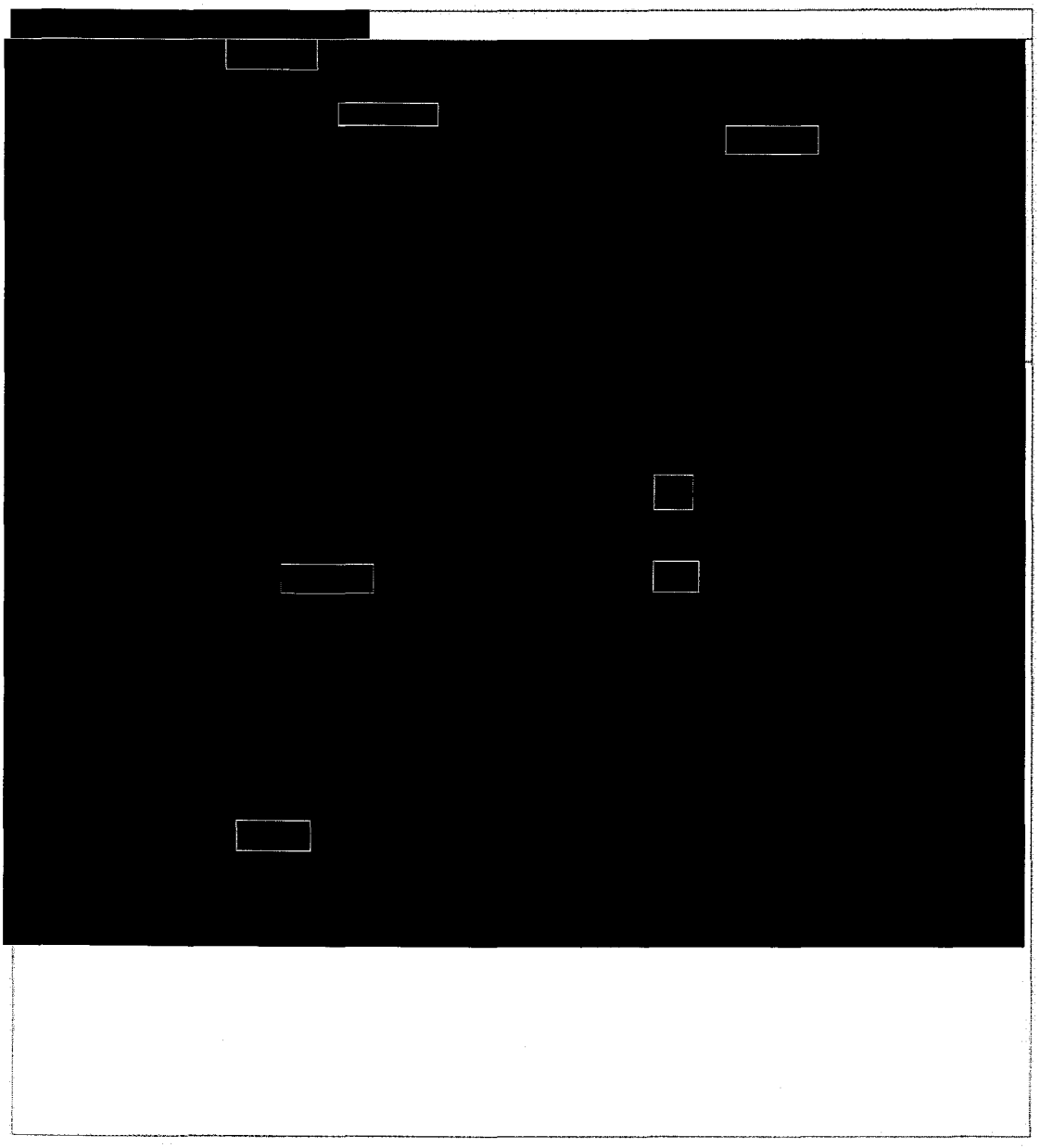


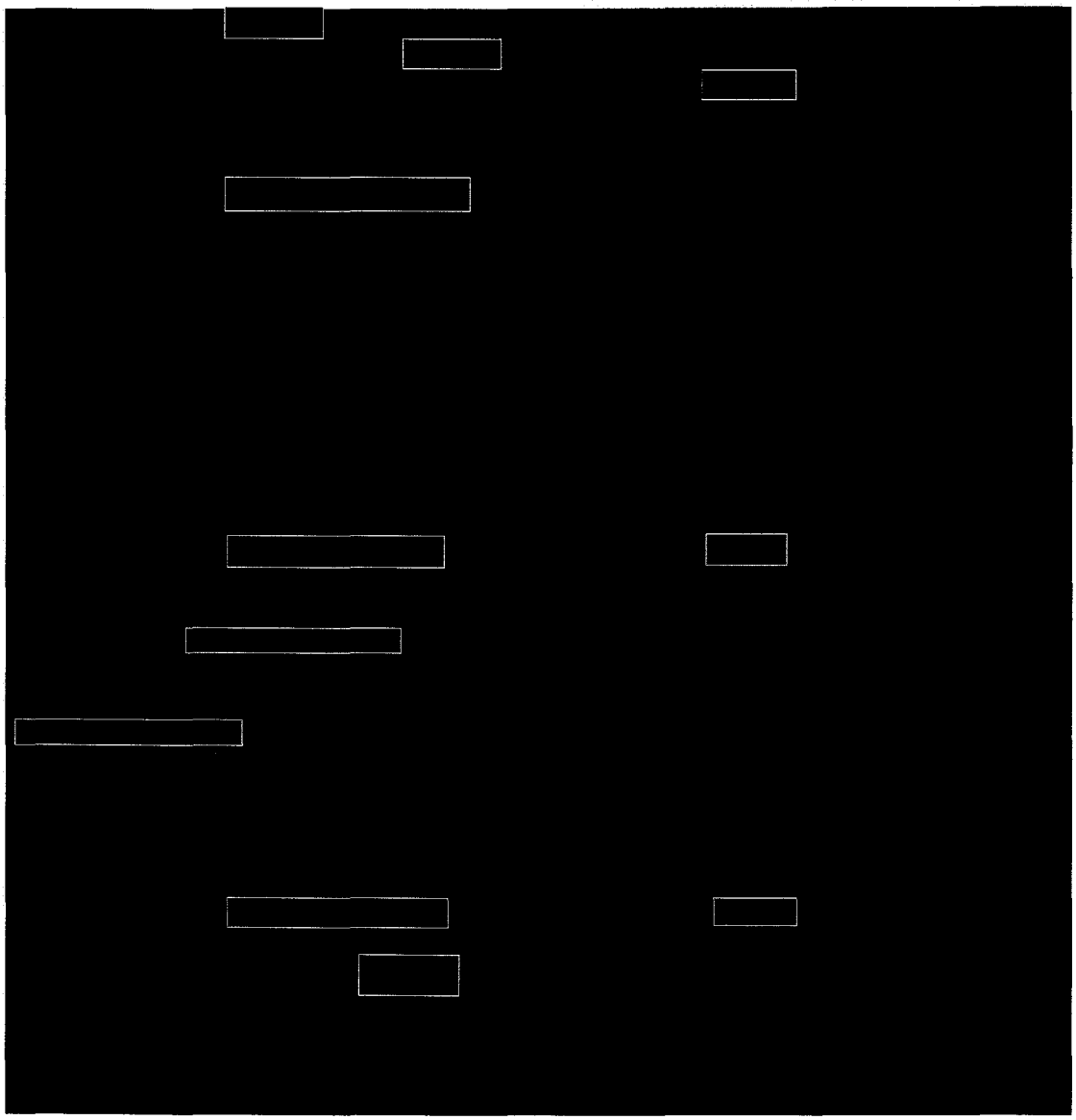
TAB

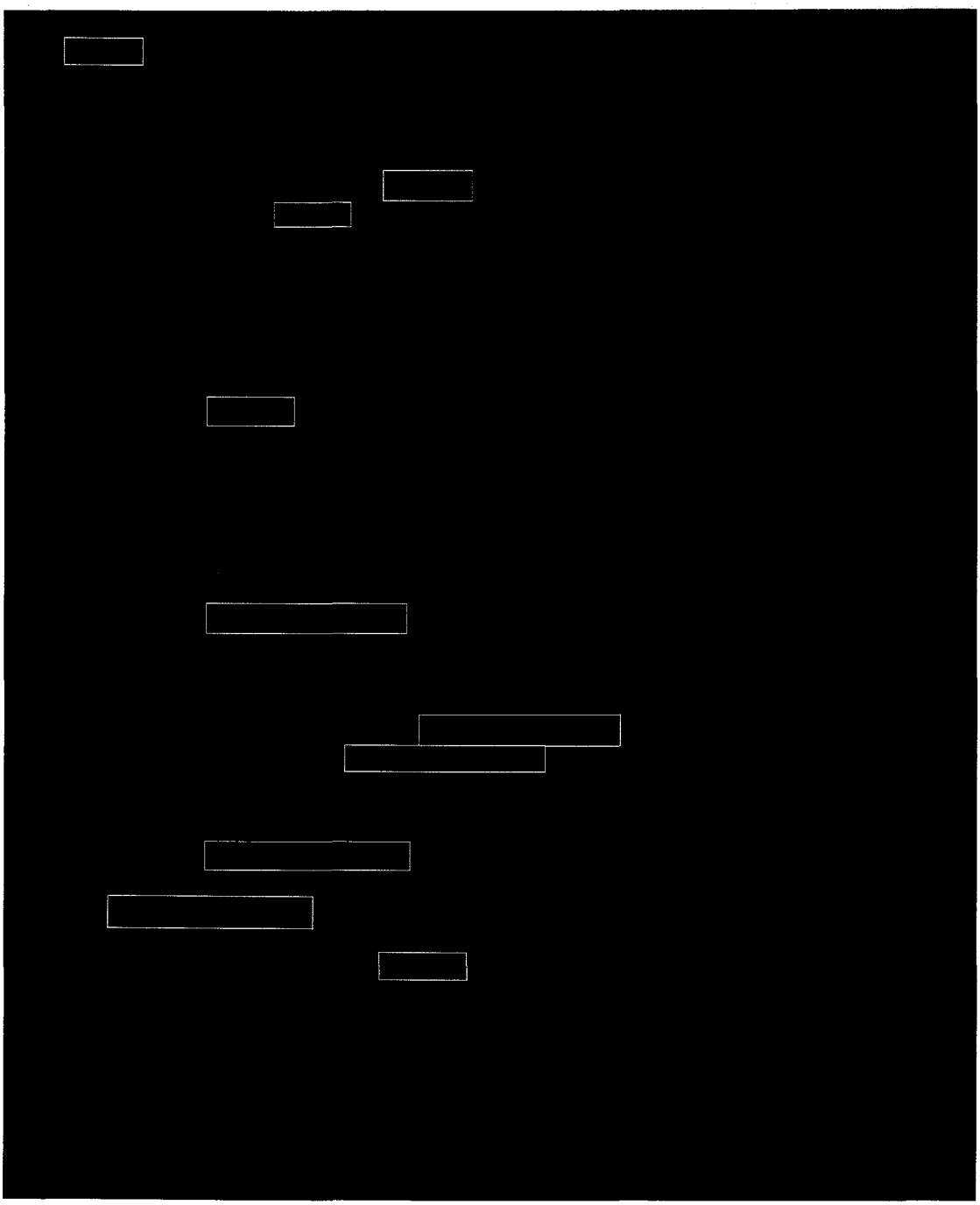
4

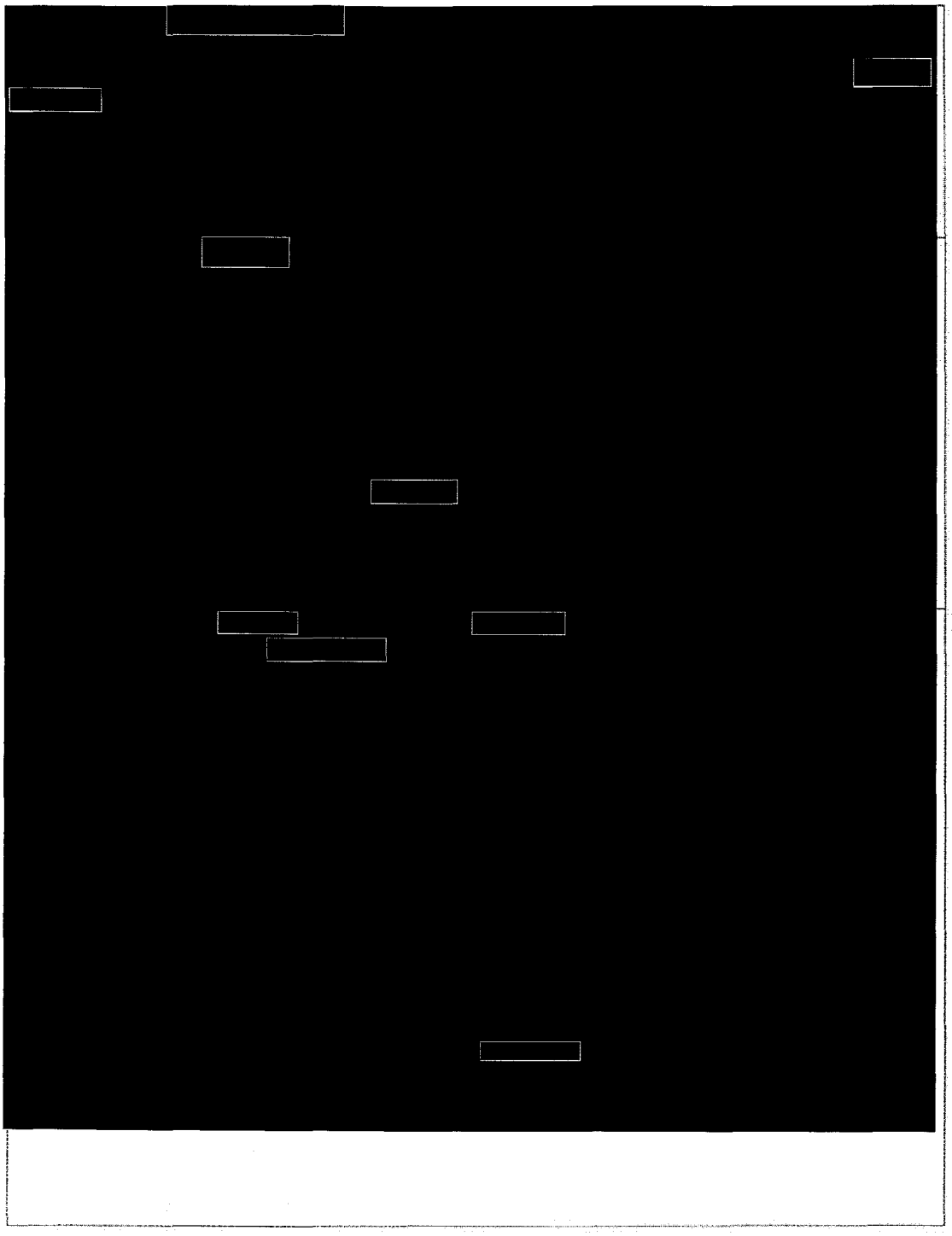
IAB NPOs related to the energy sector
2009 12 31 to 2015 07 30

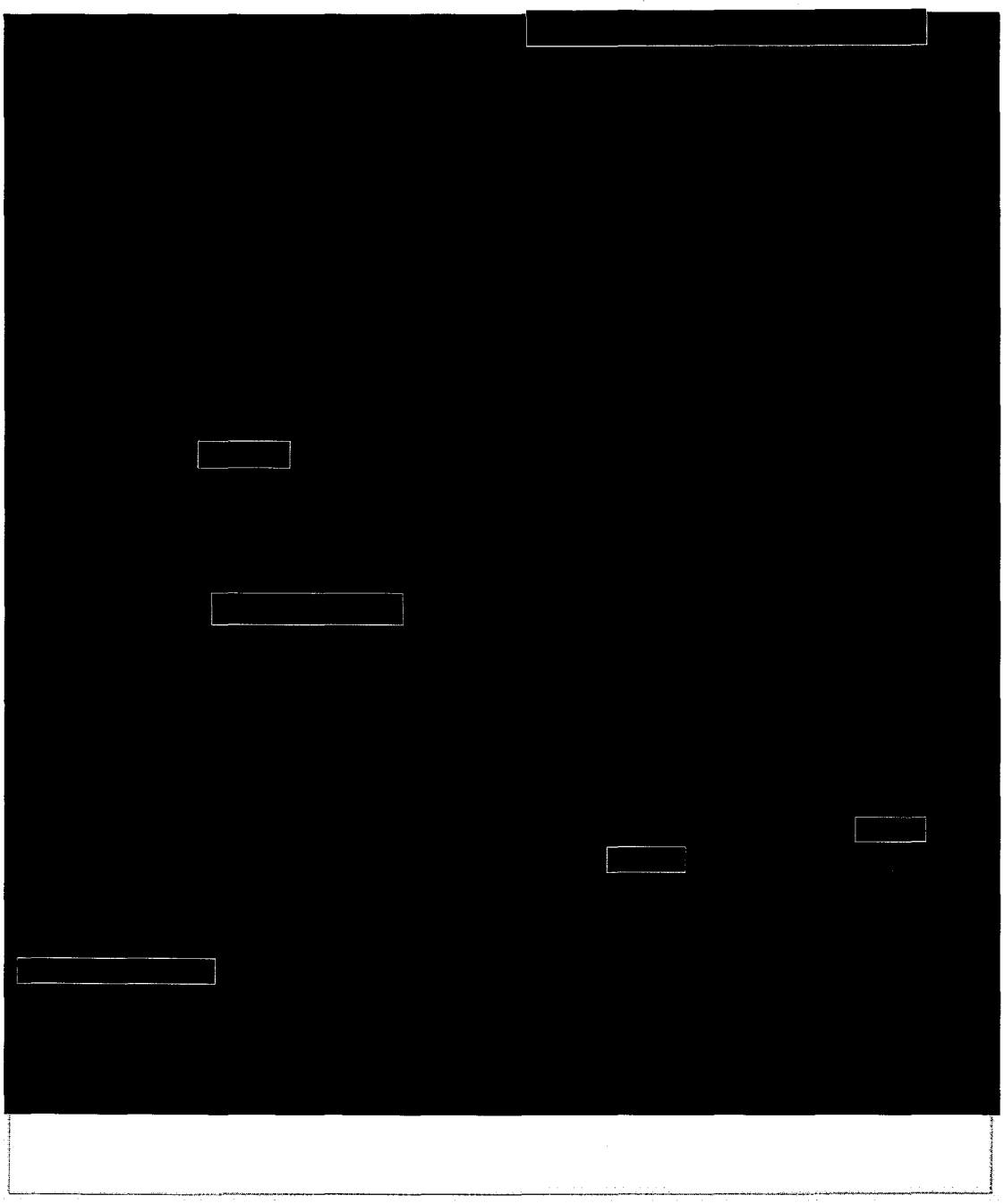
[redacted] exported from Excel to Word)

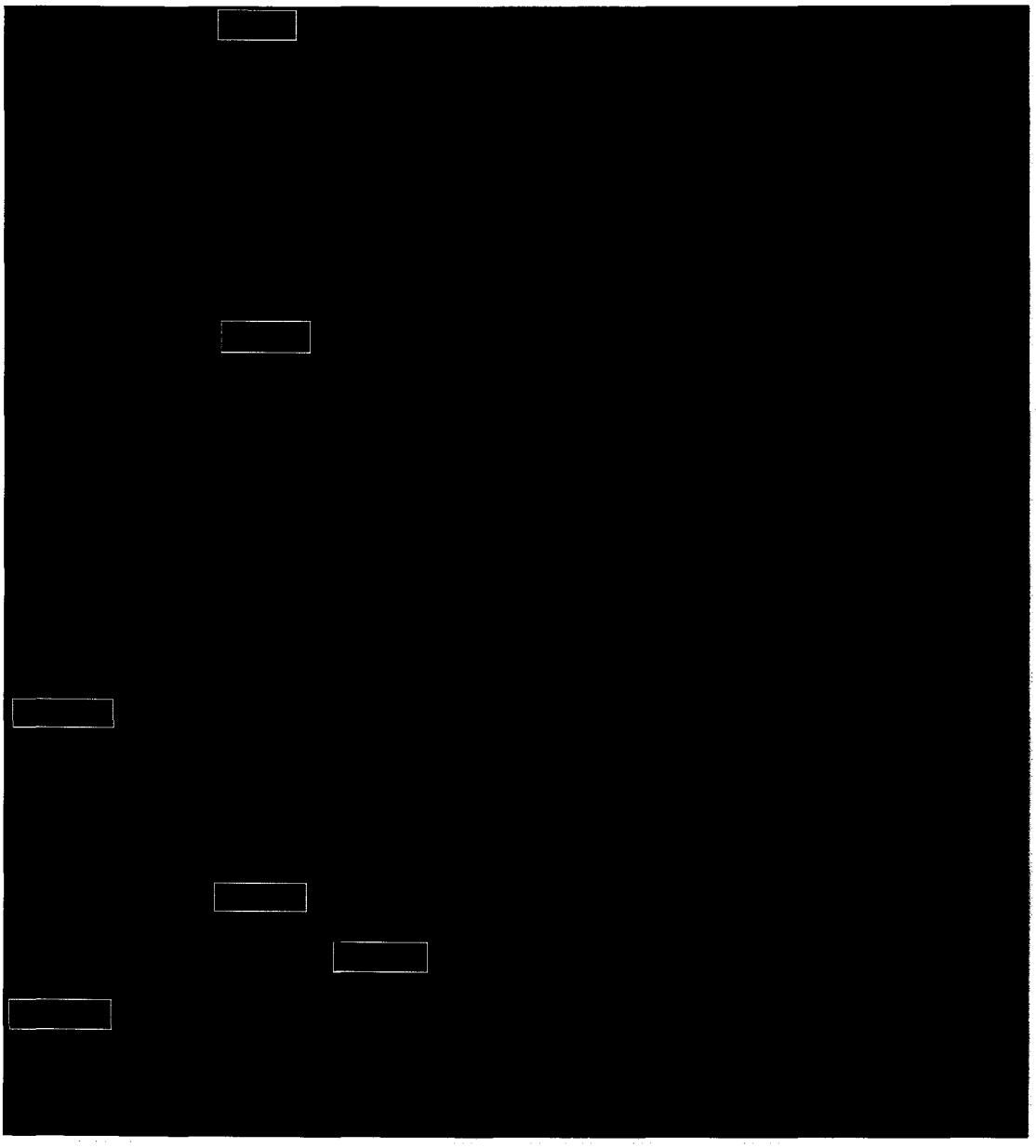


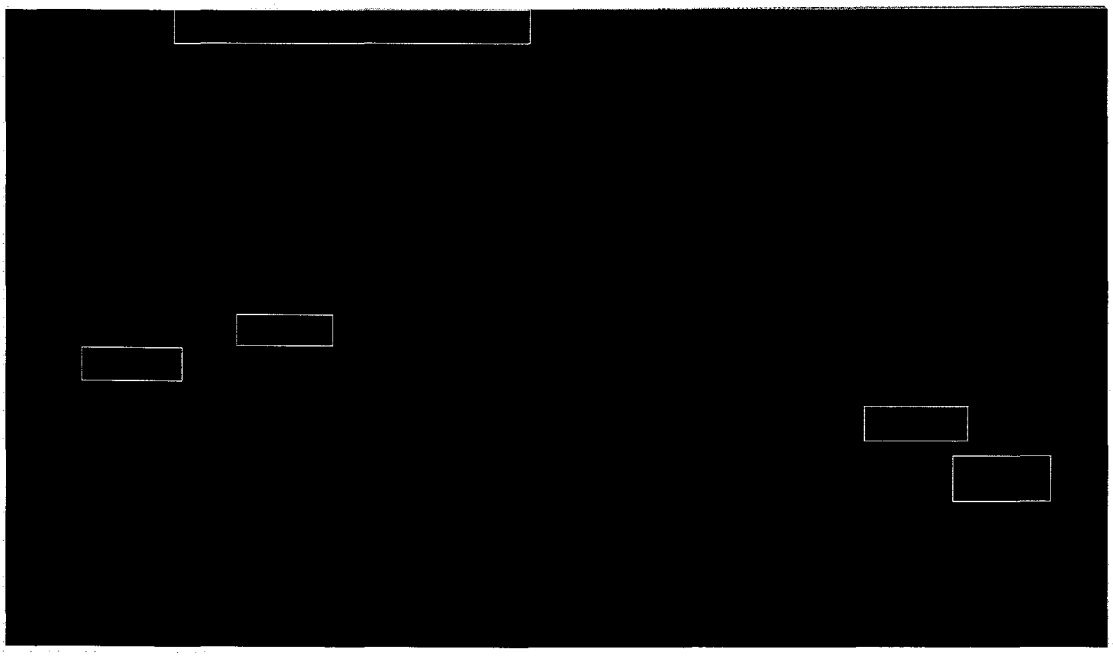


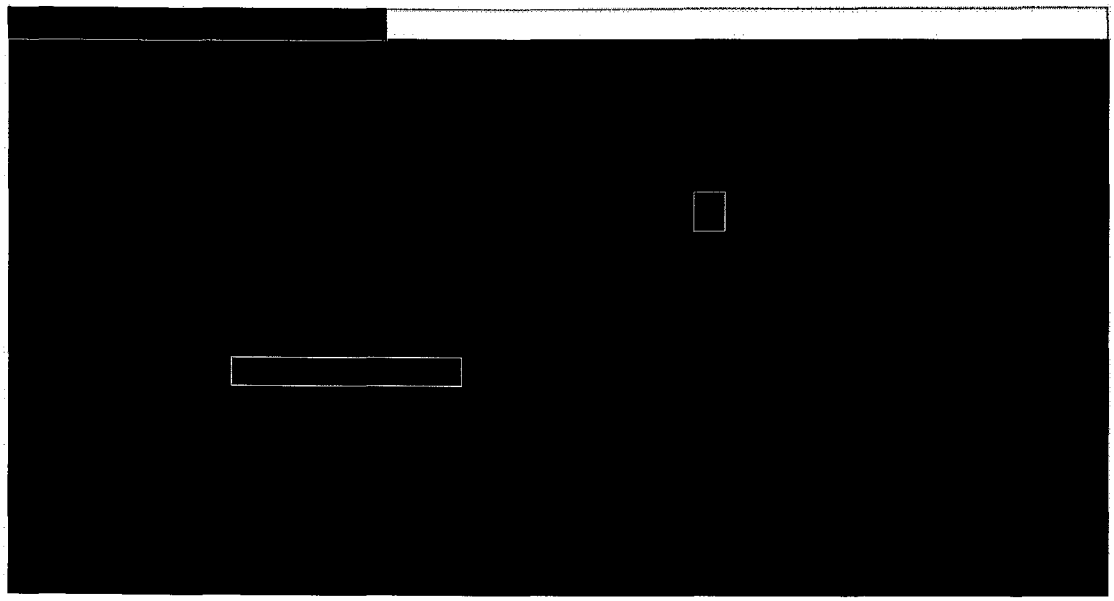


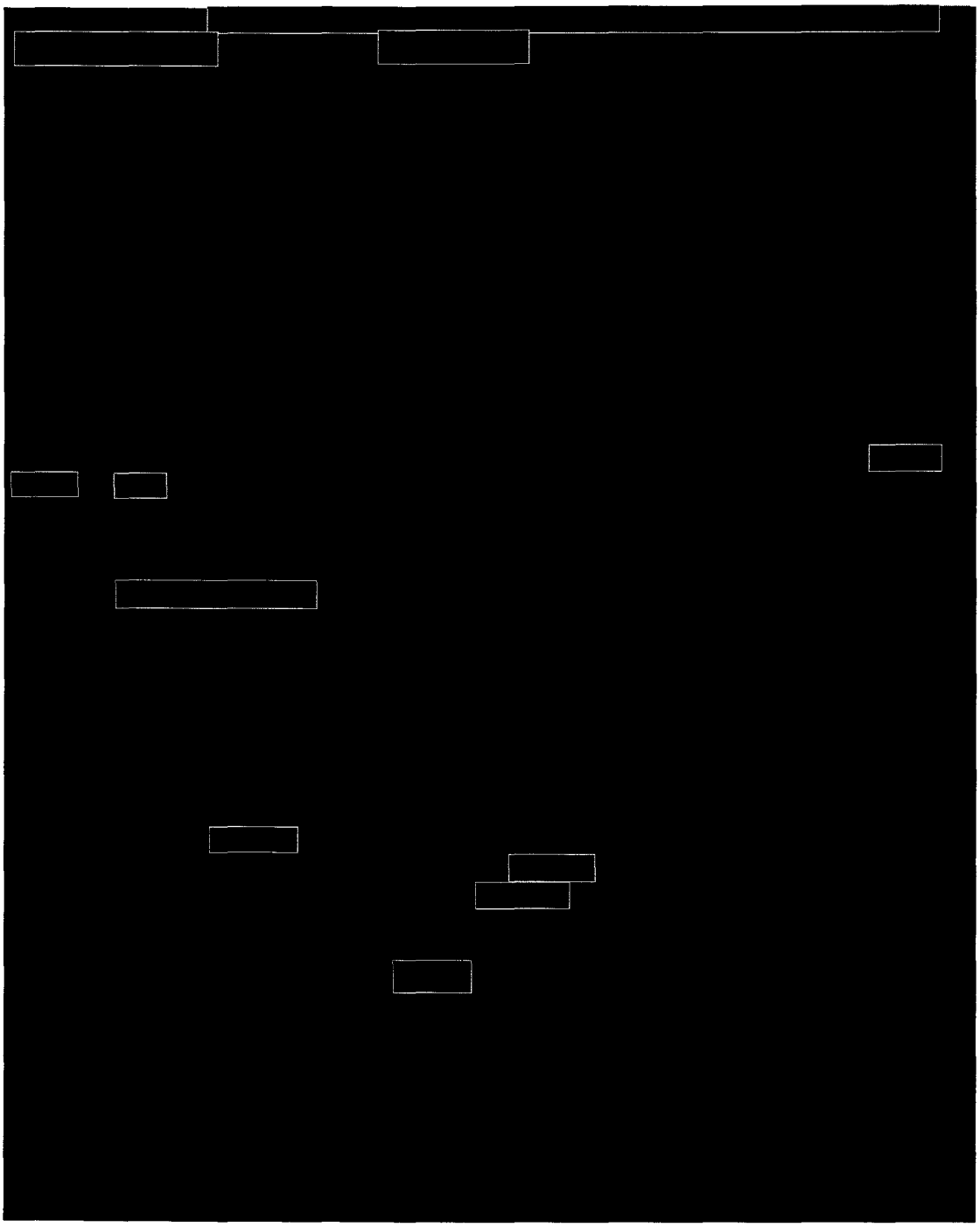


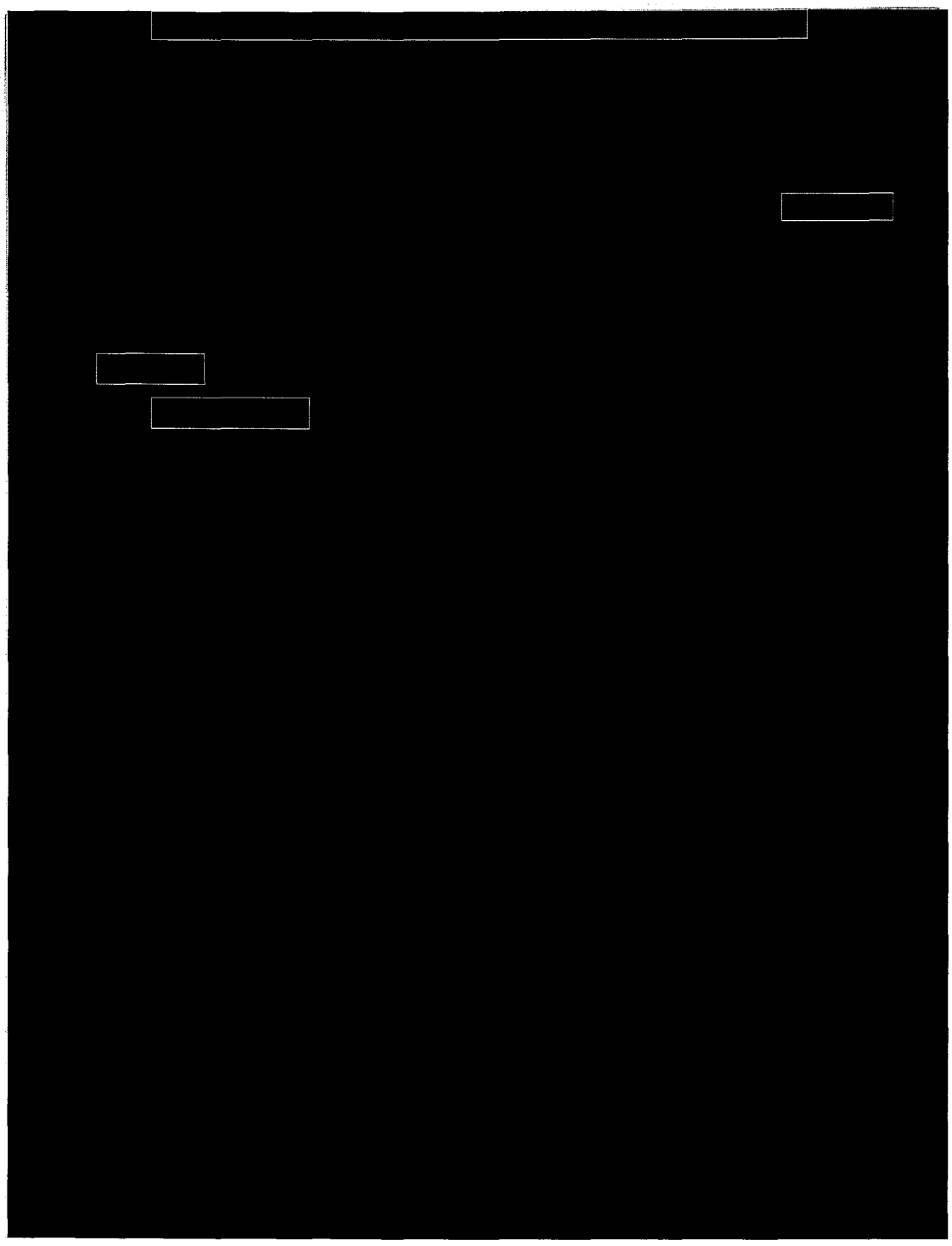


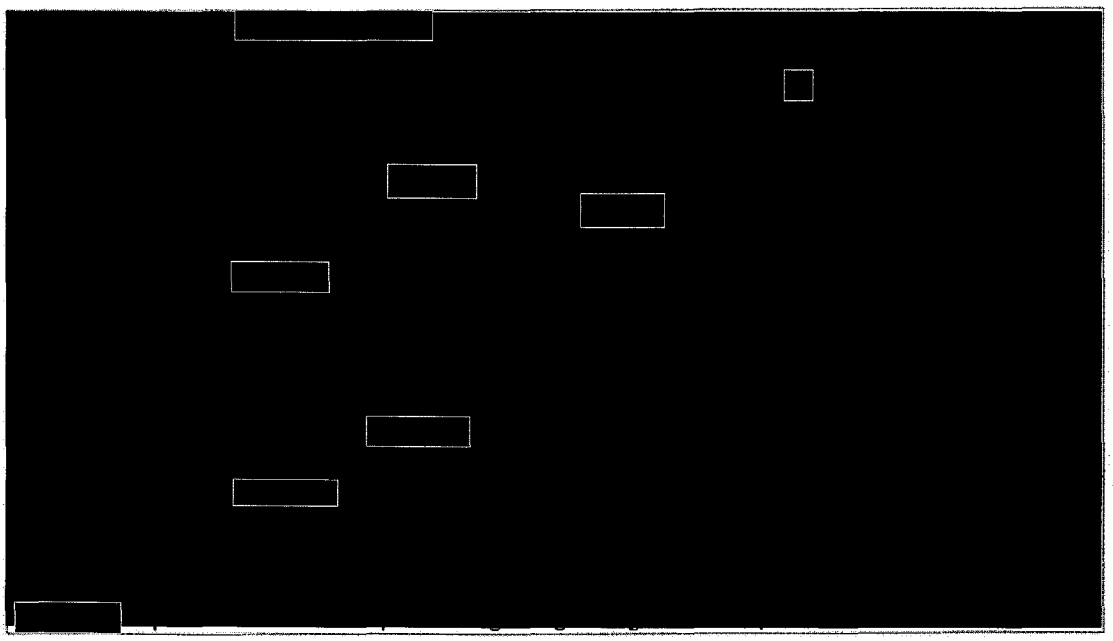


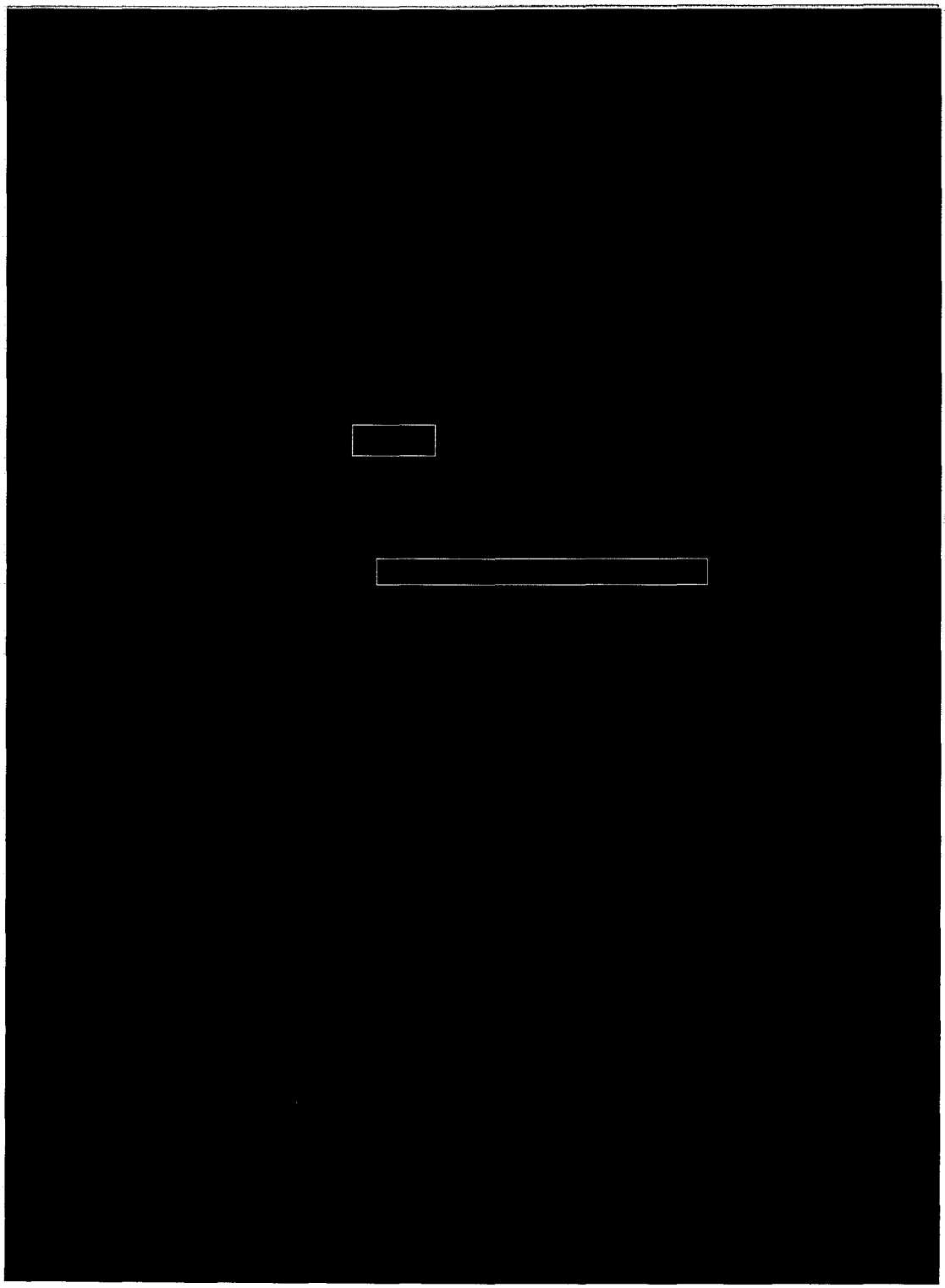


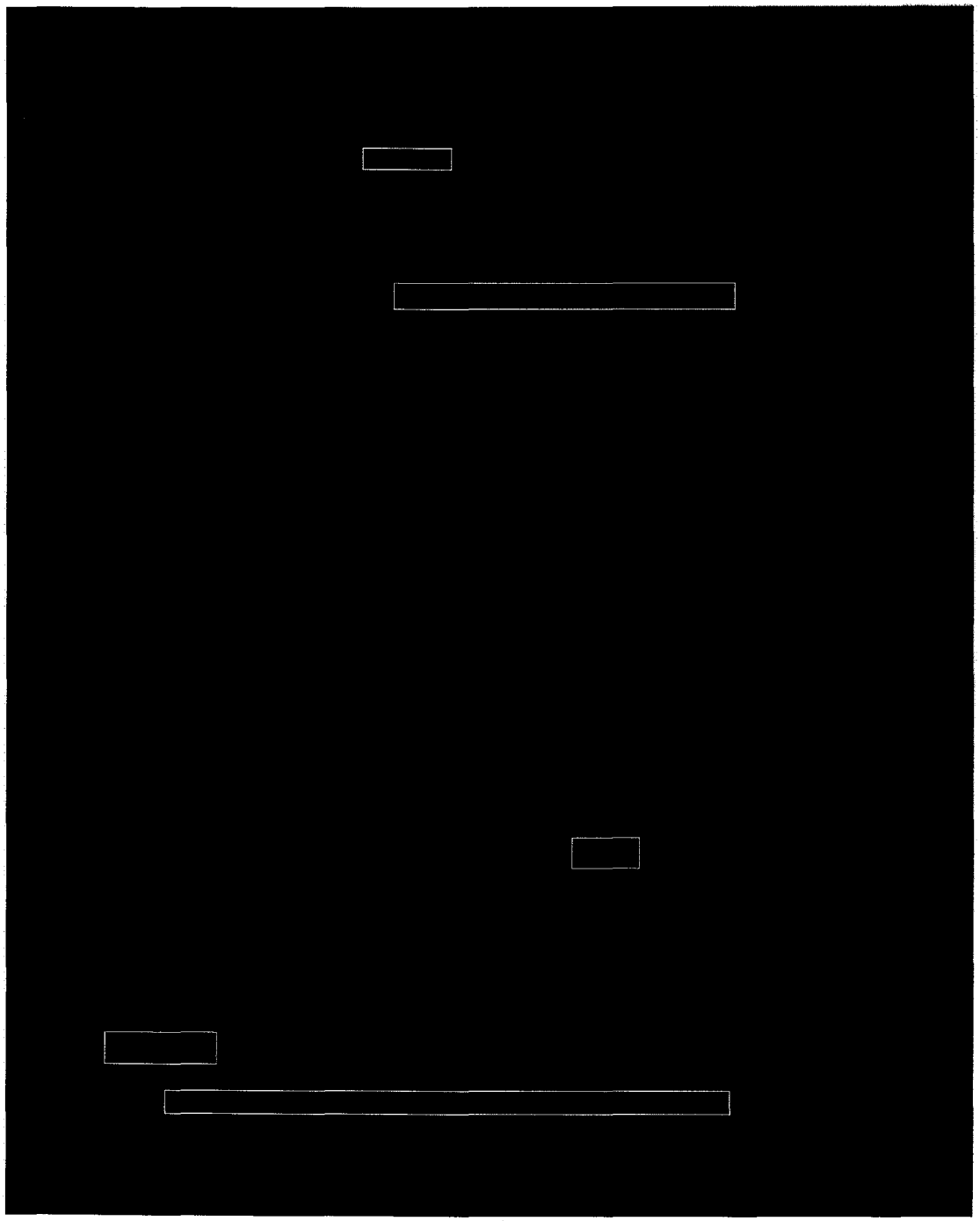


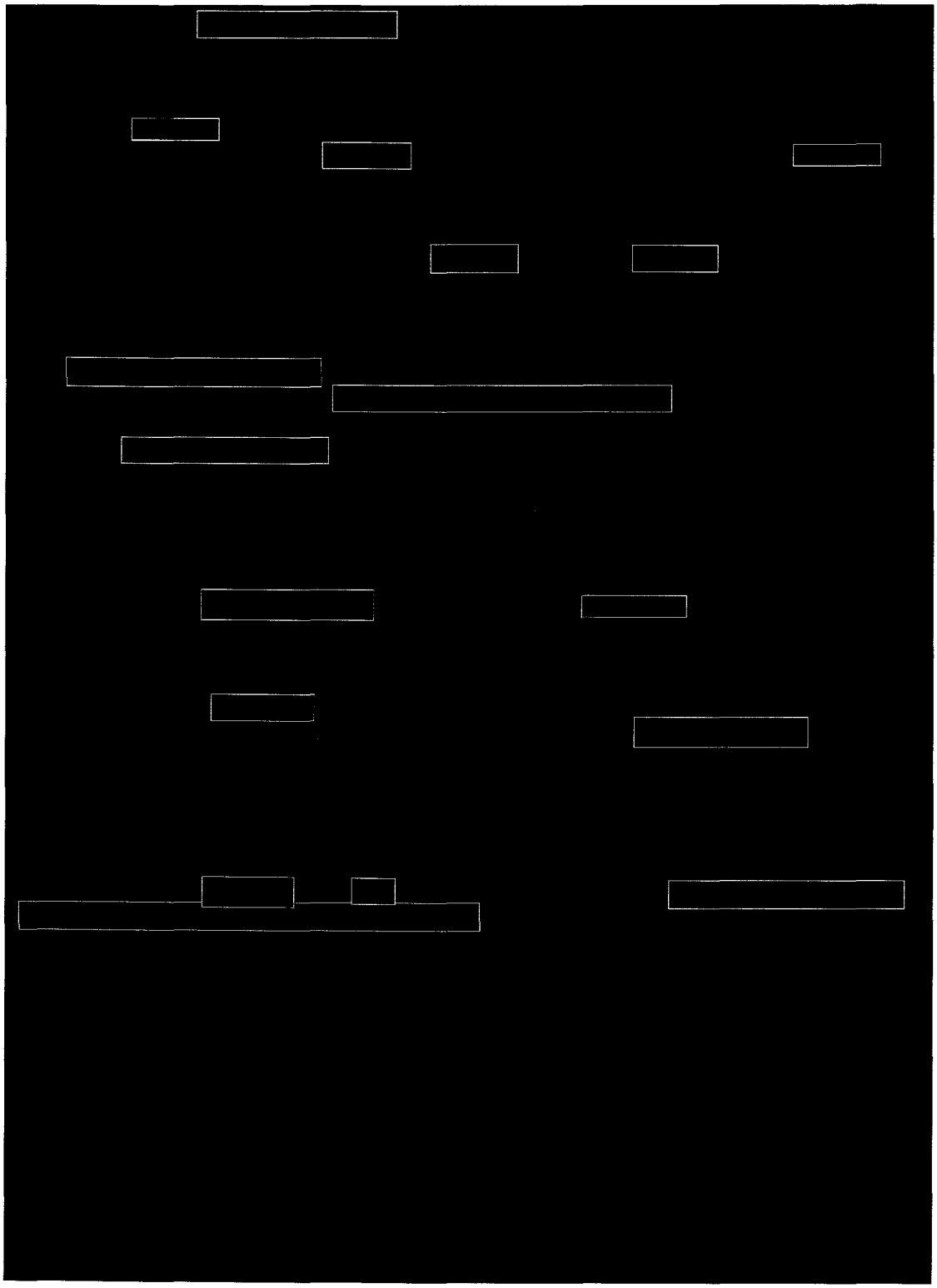


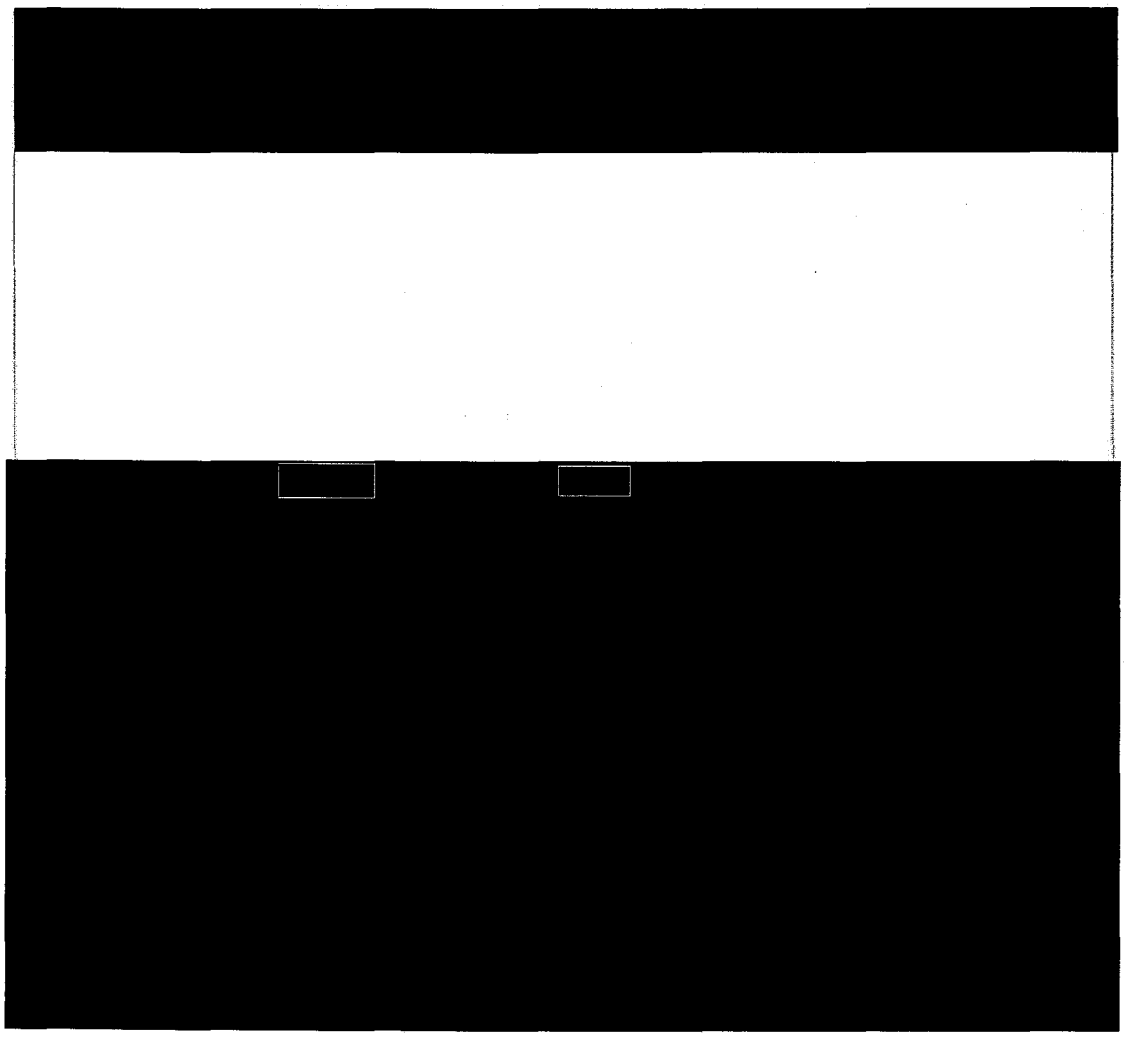


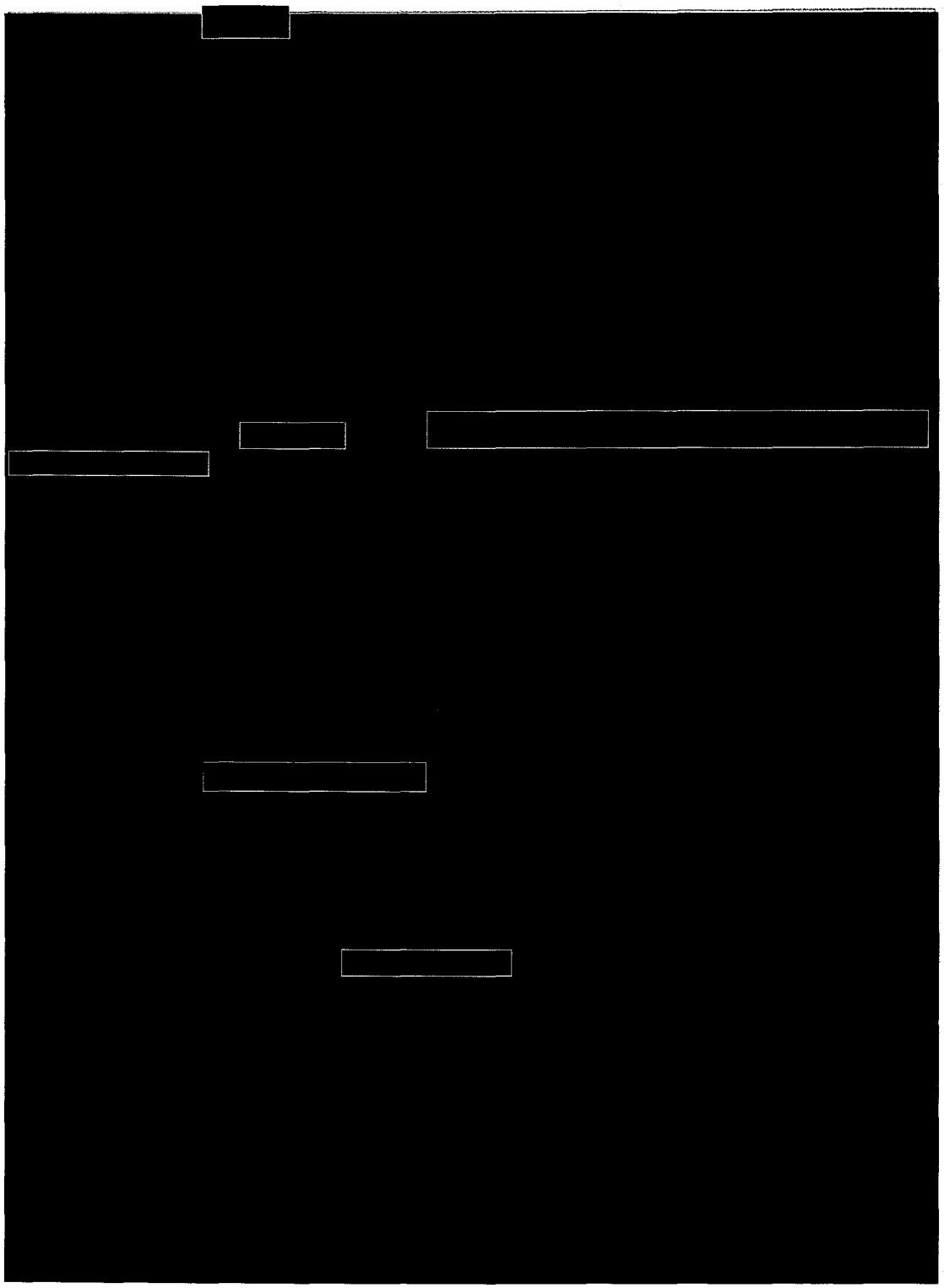


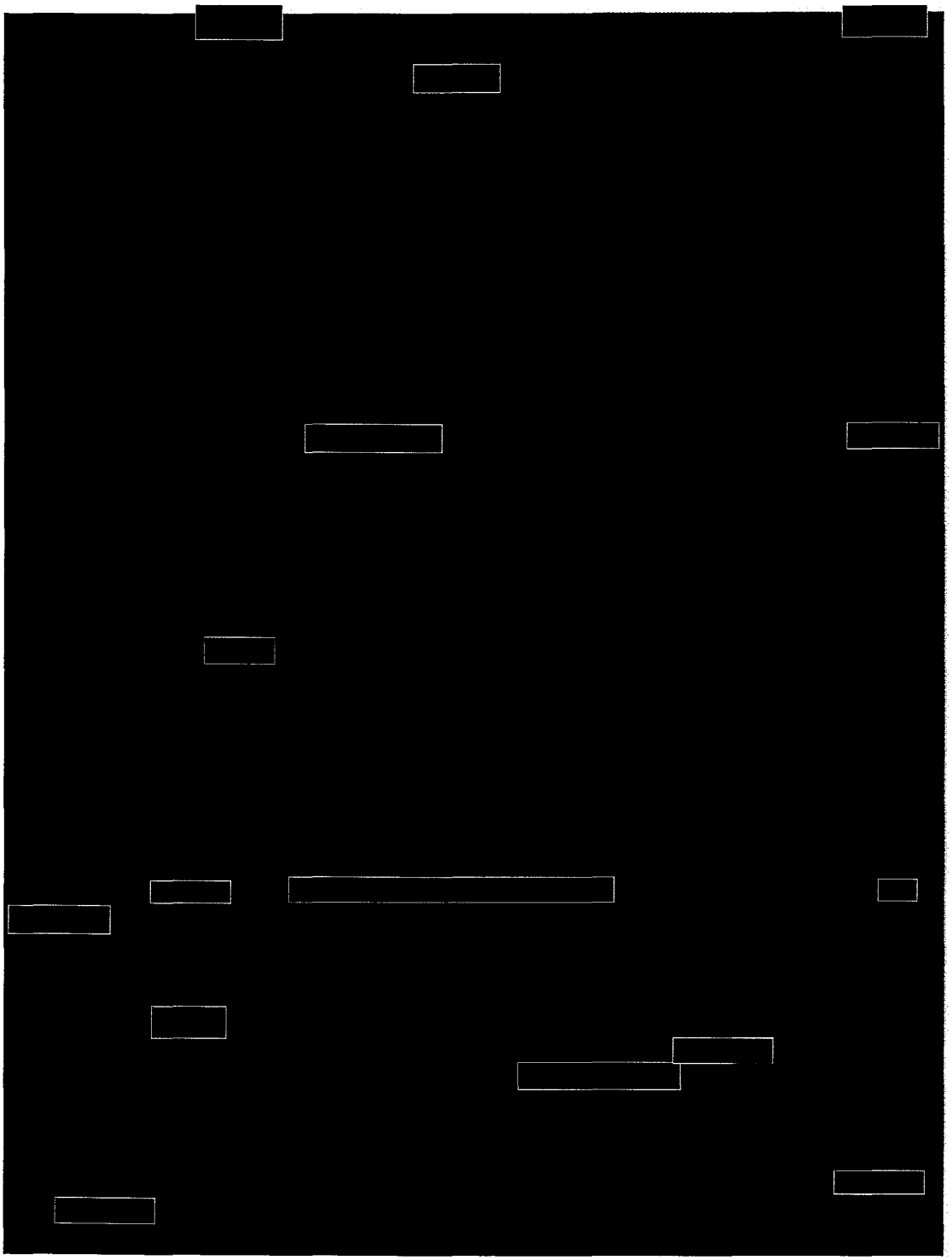


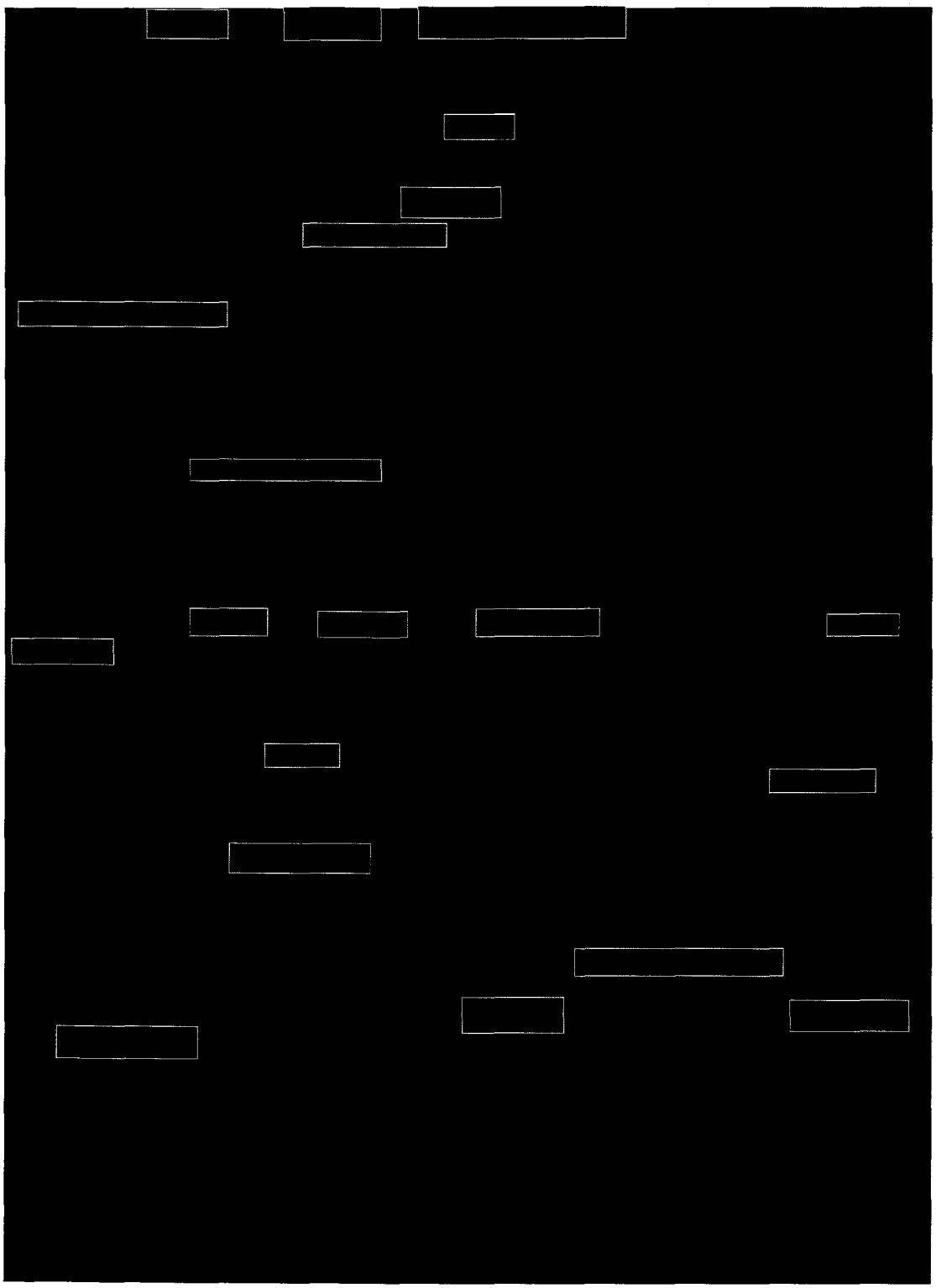


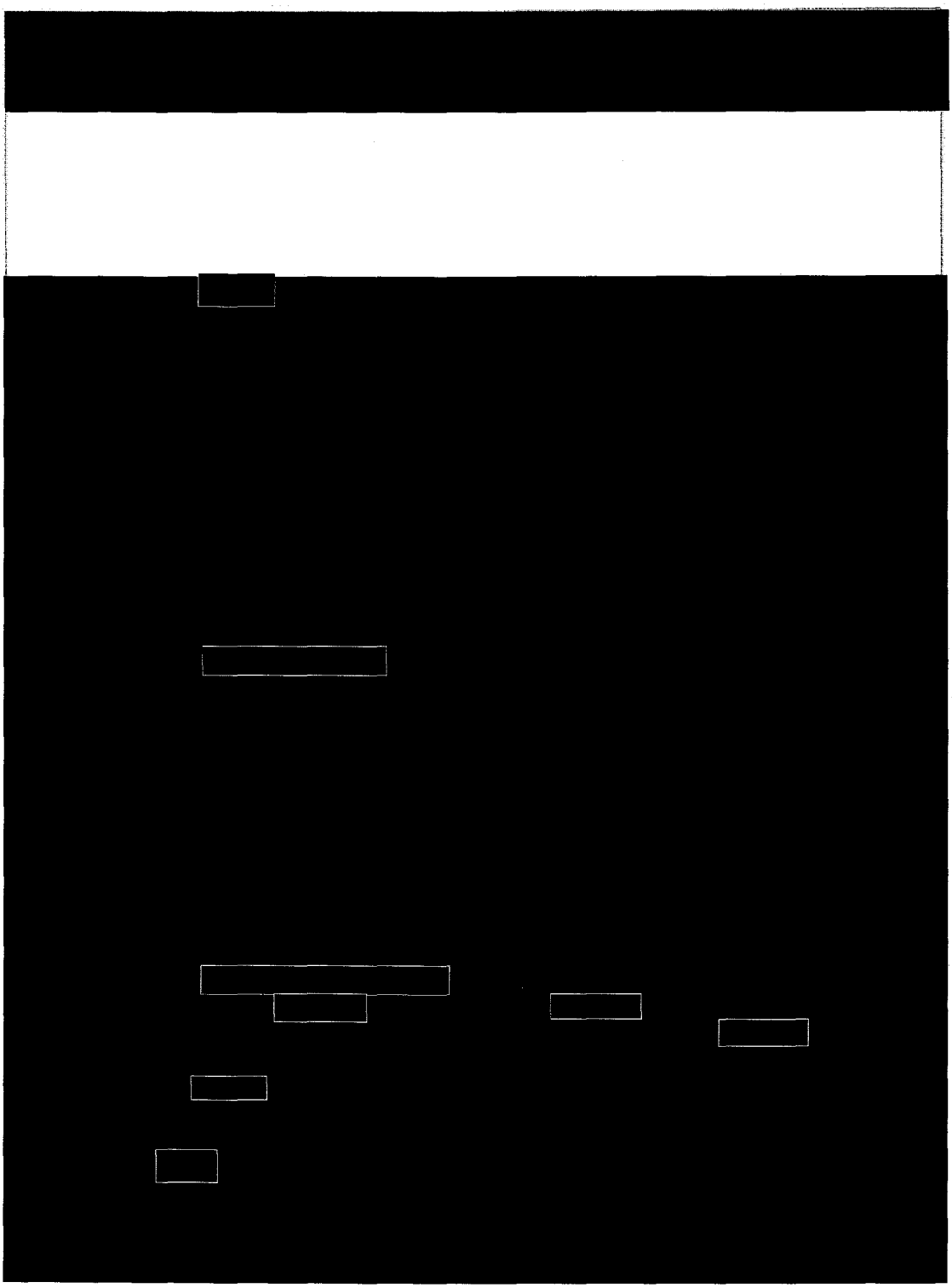


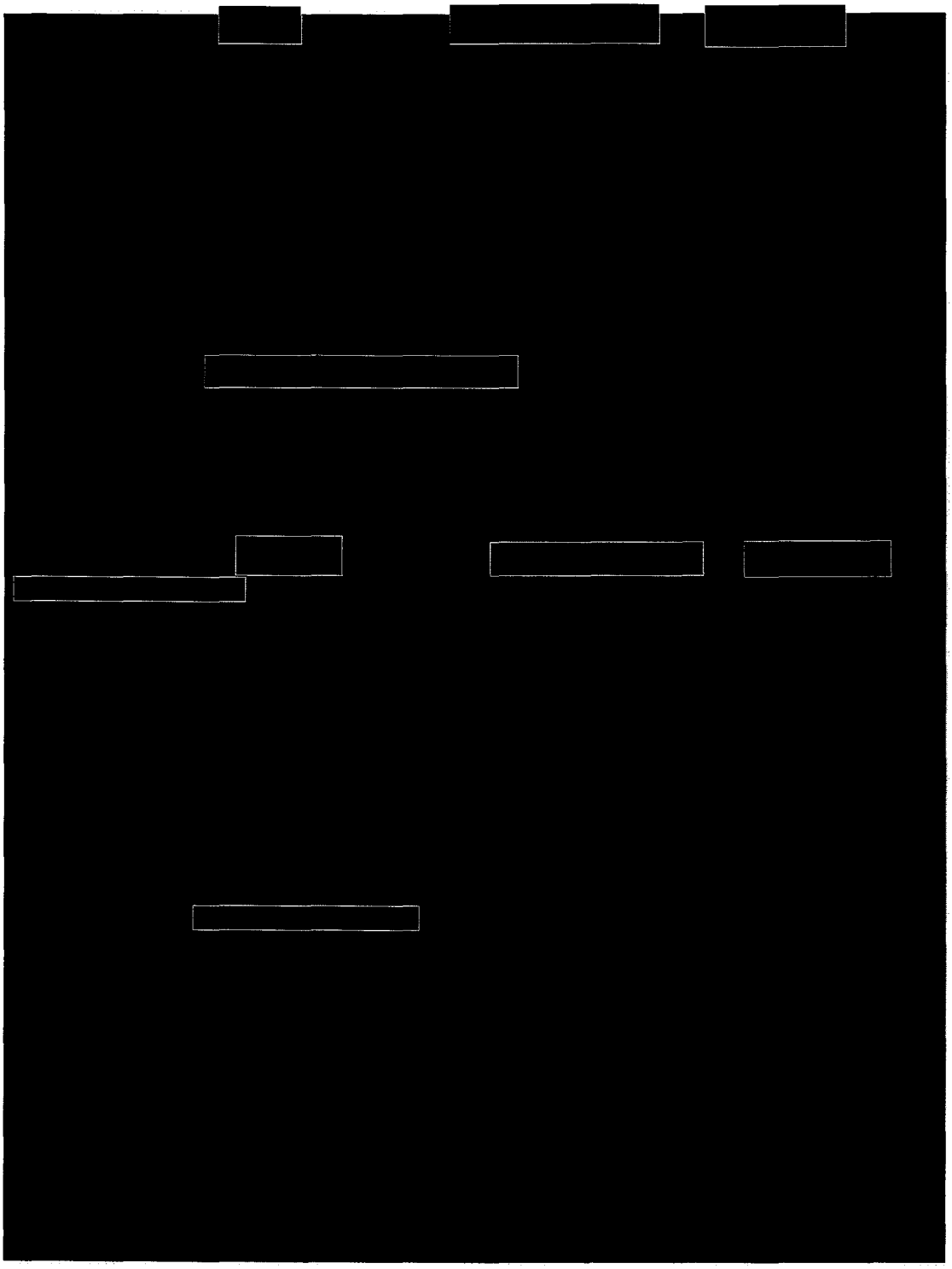


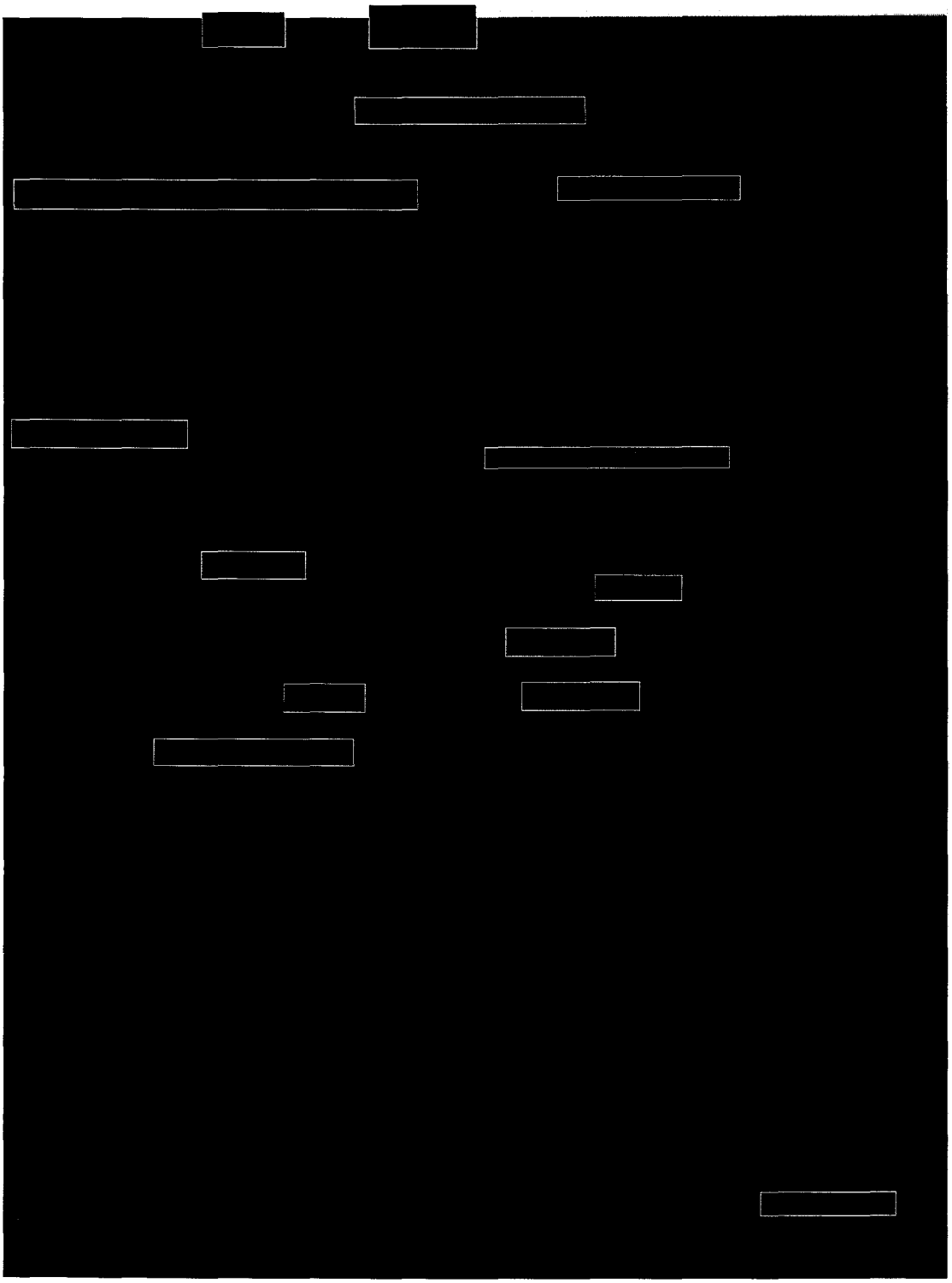


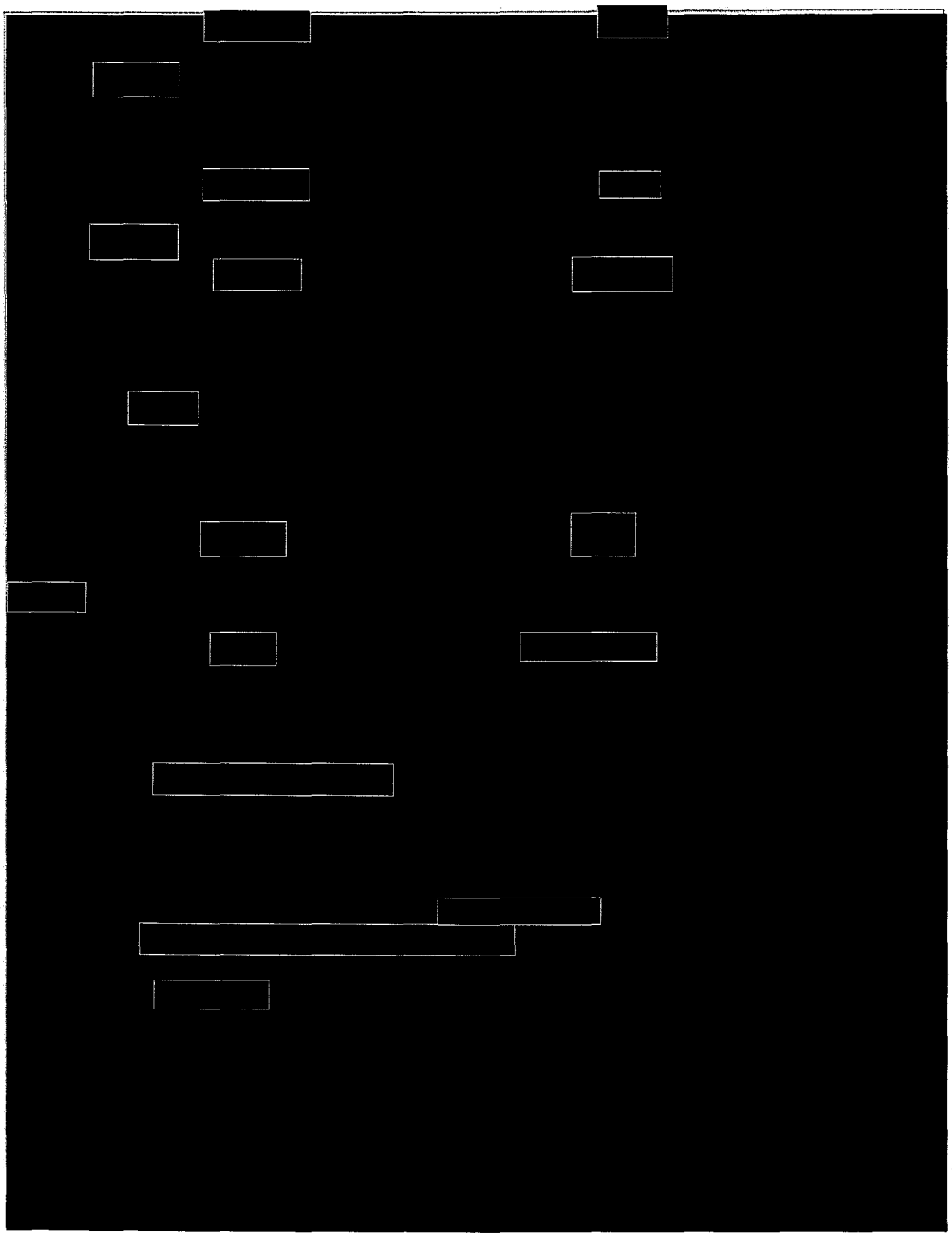


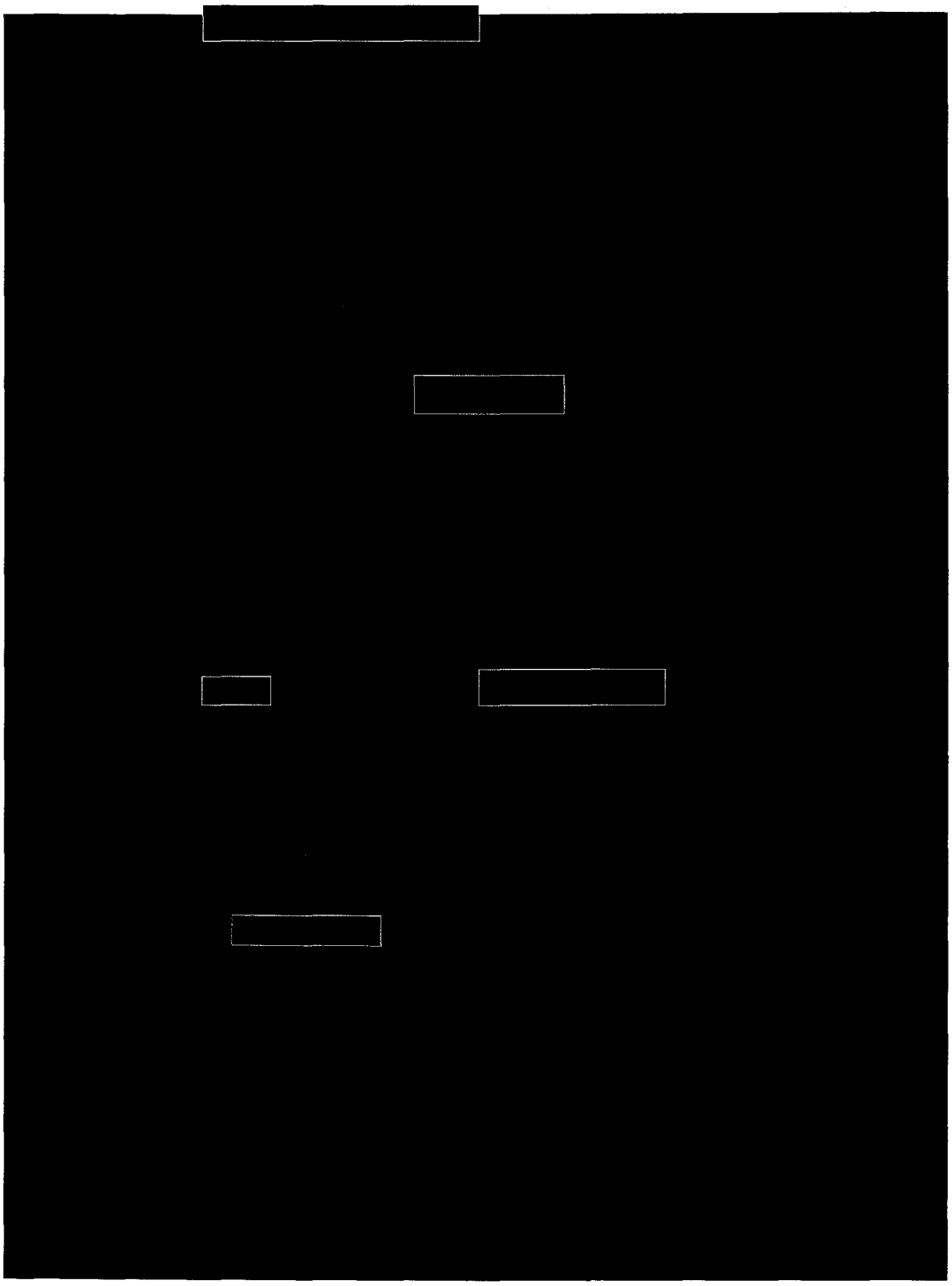


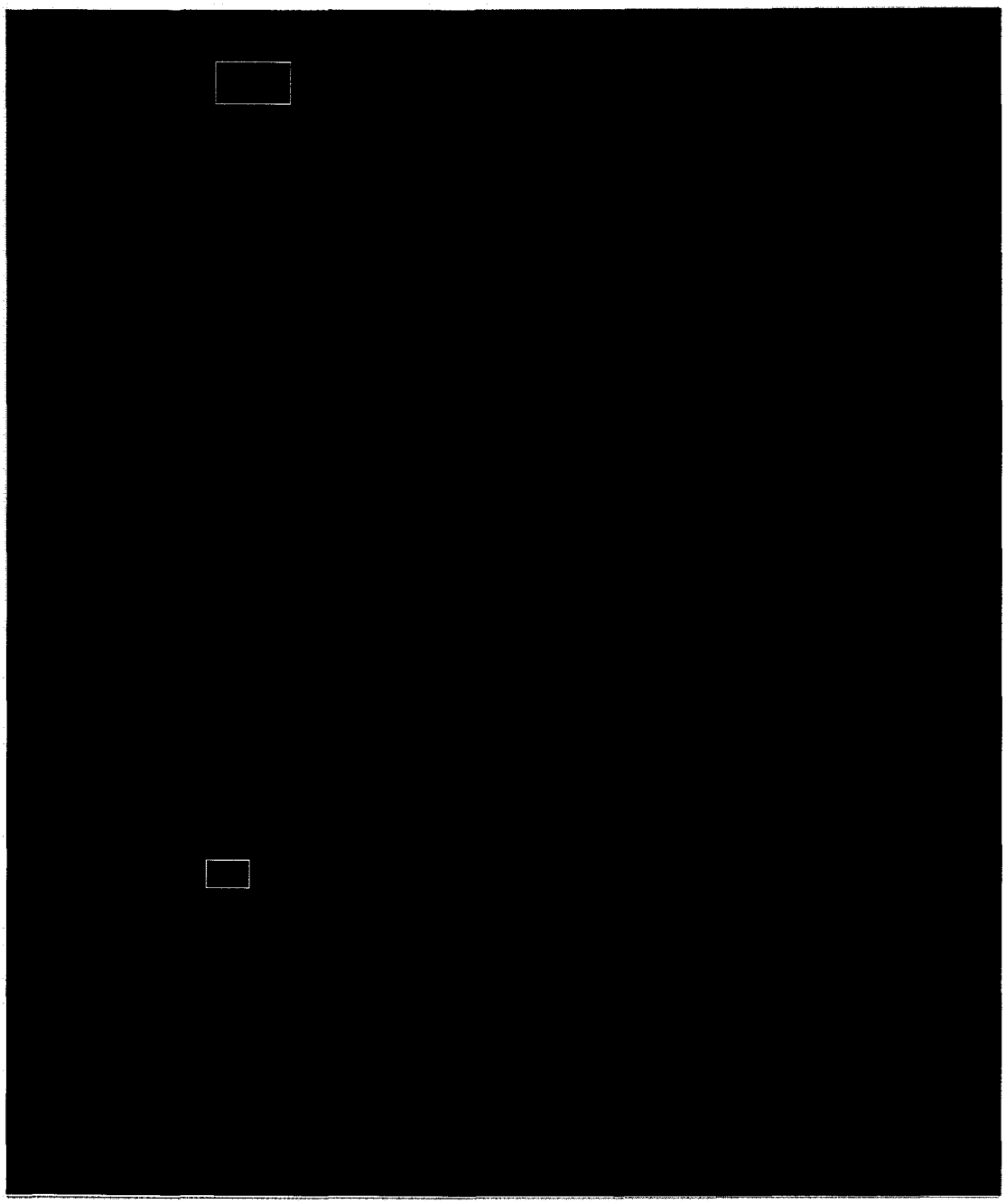


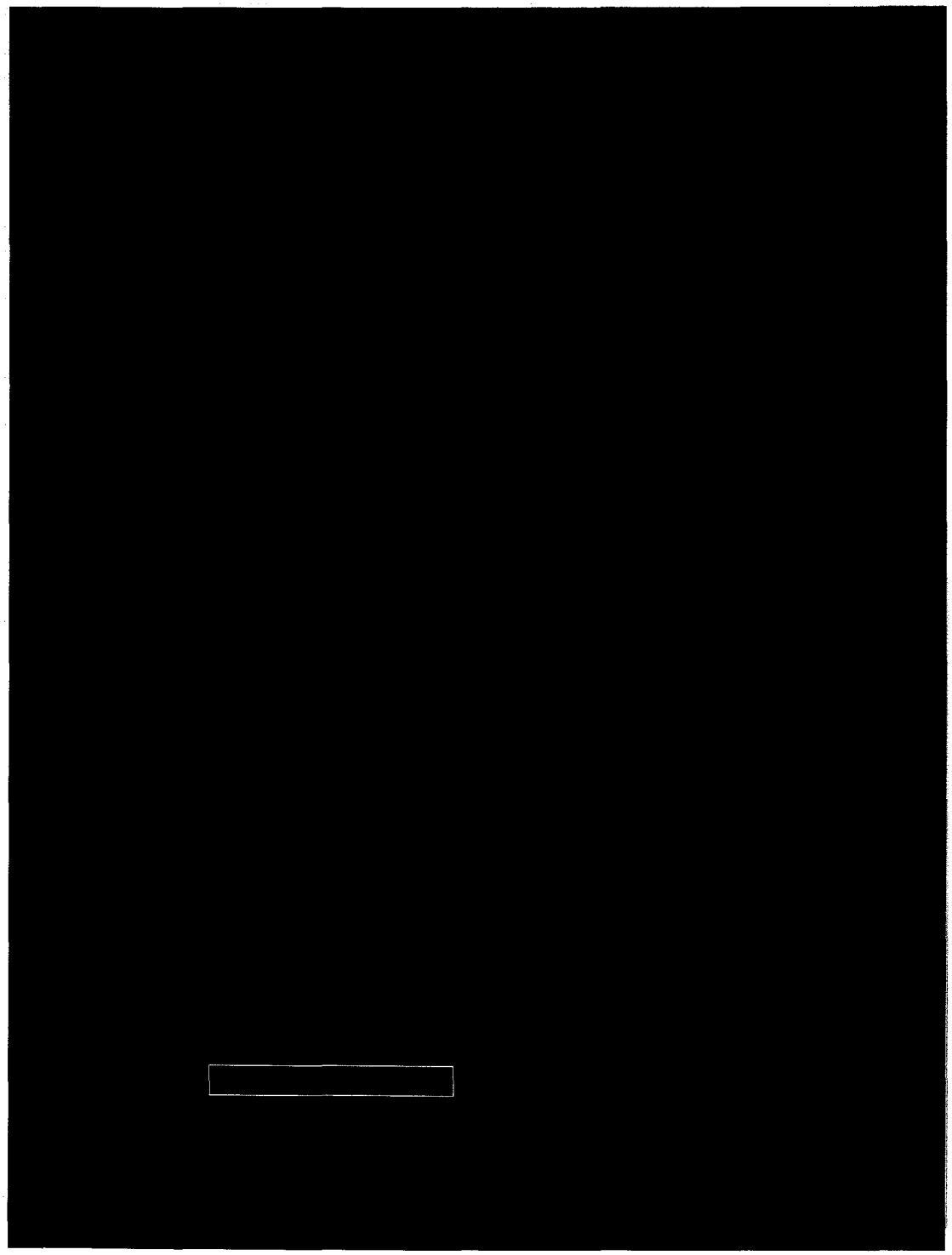


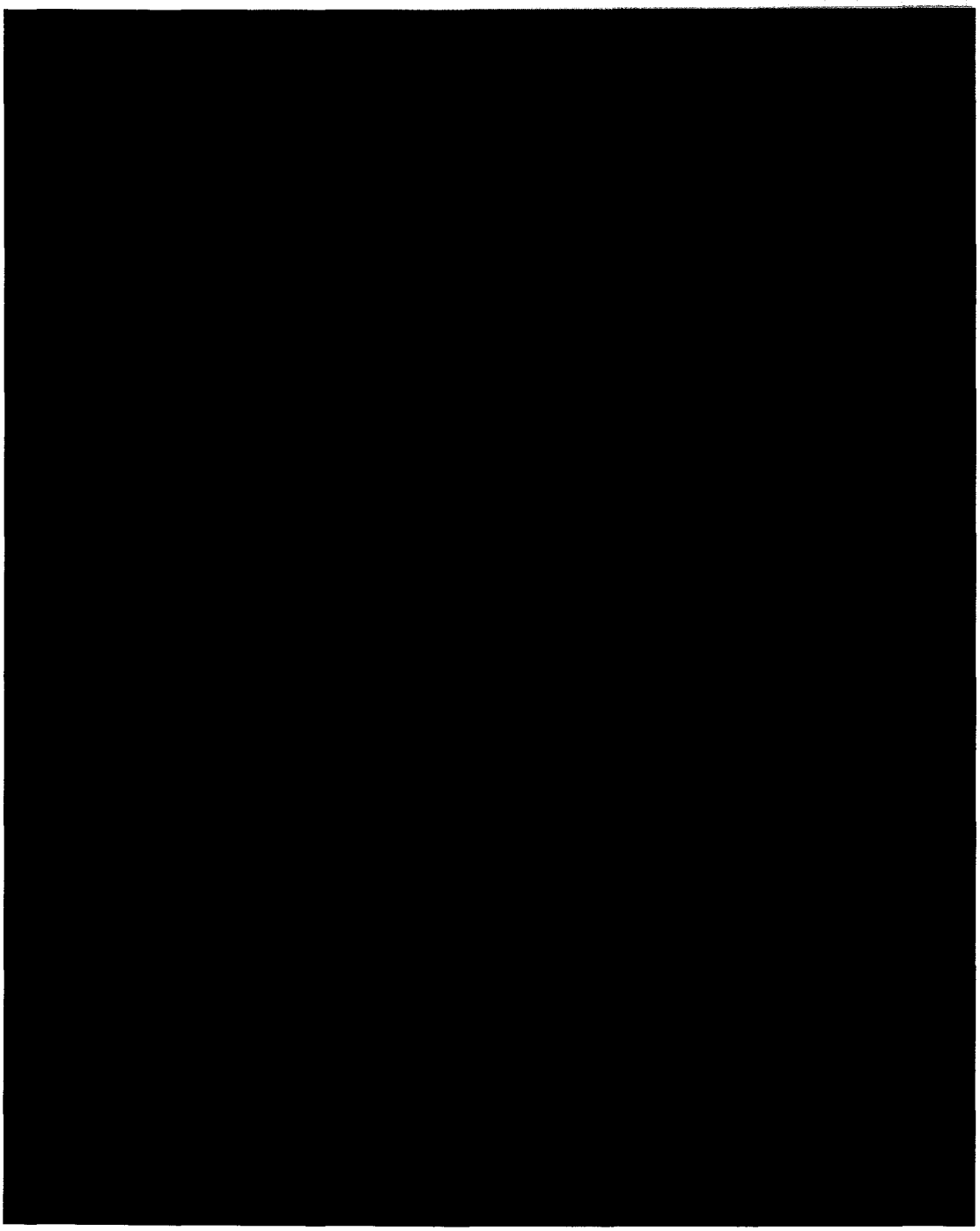


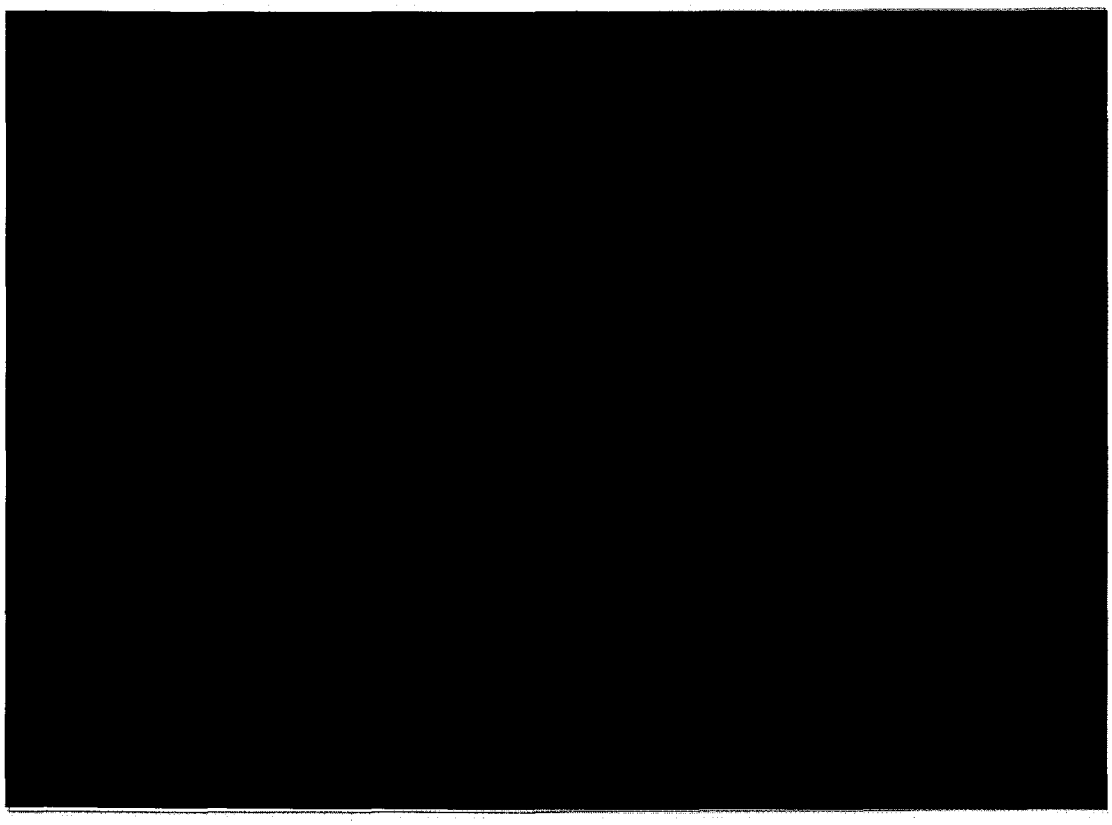










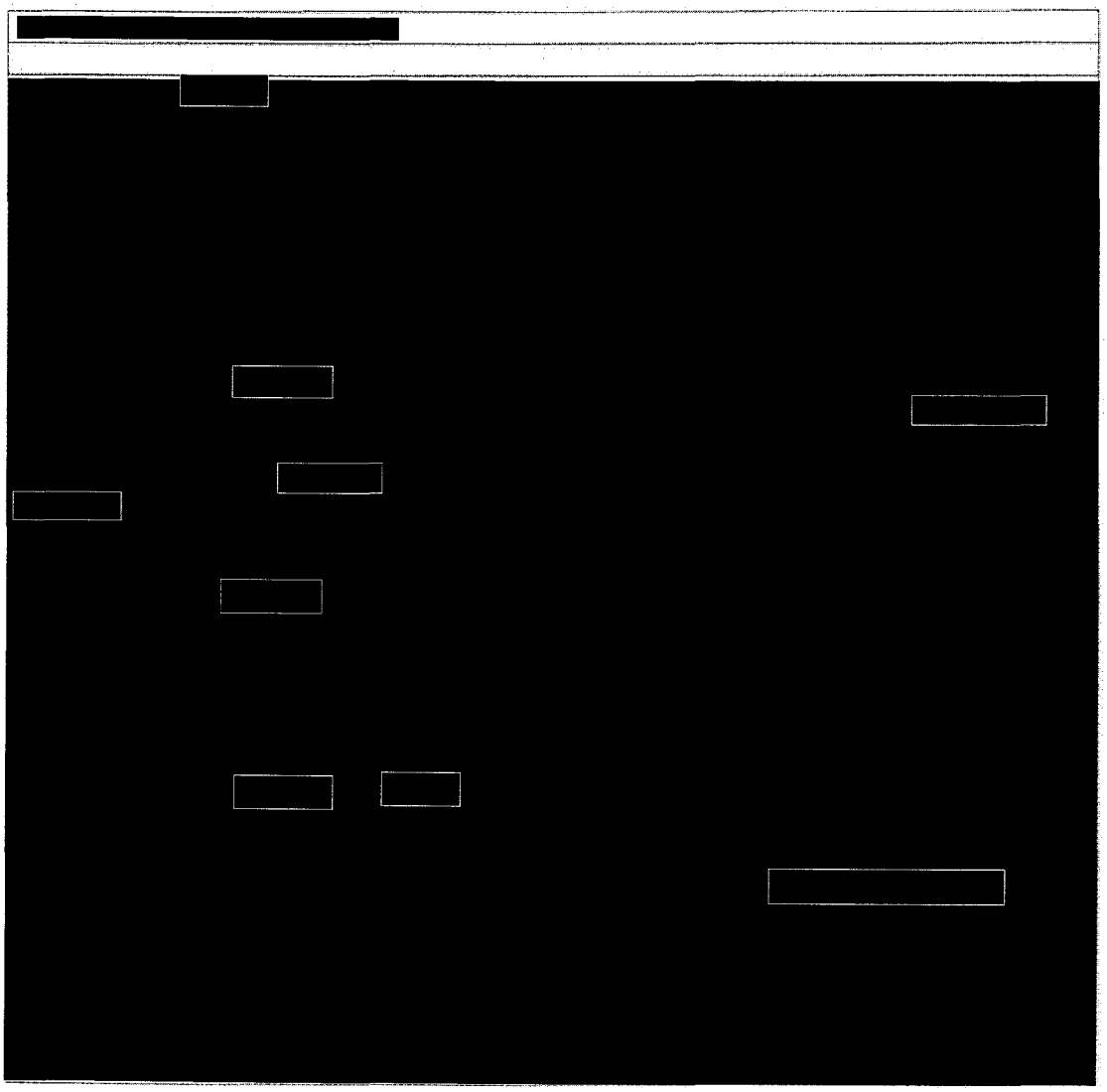


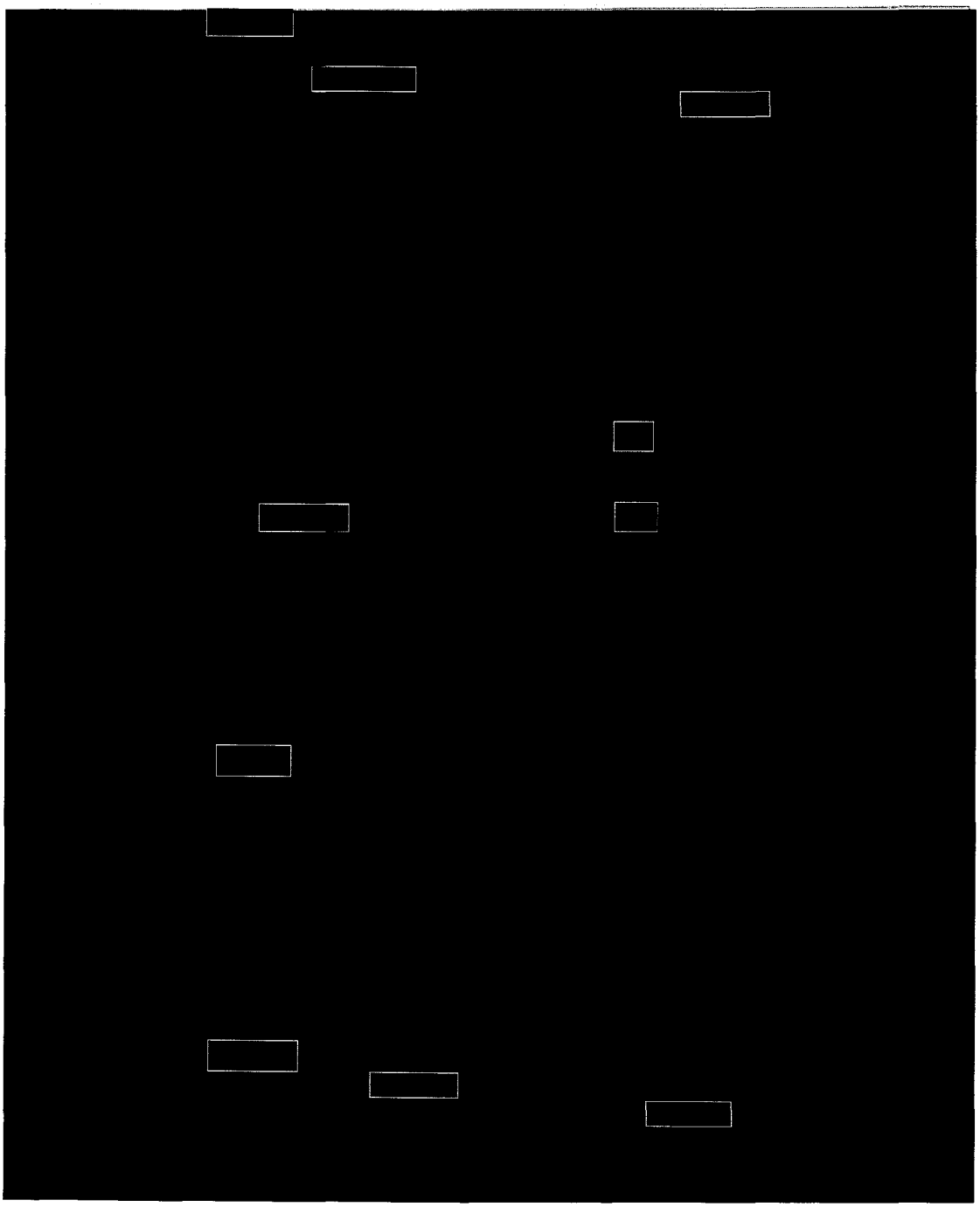
TAB

5

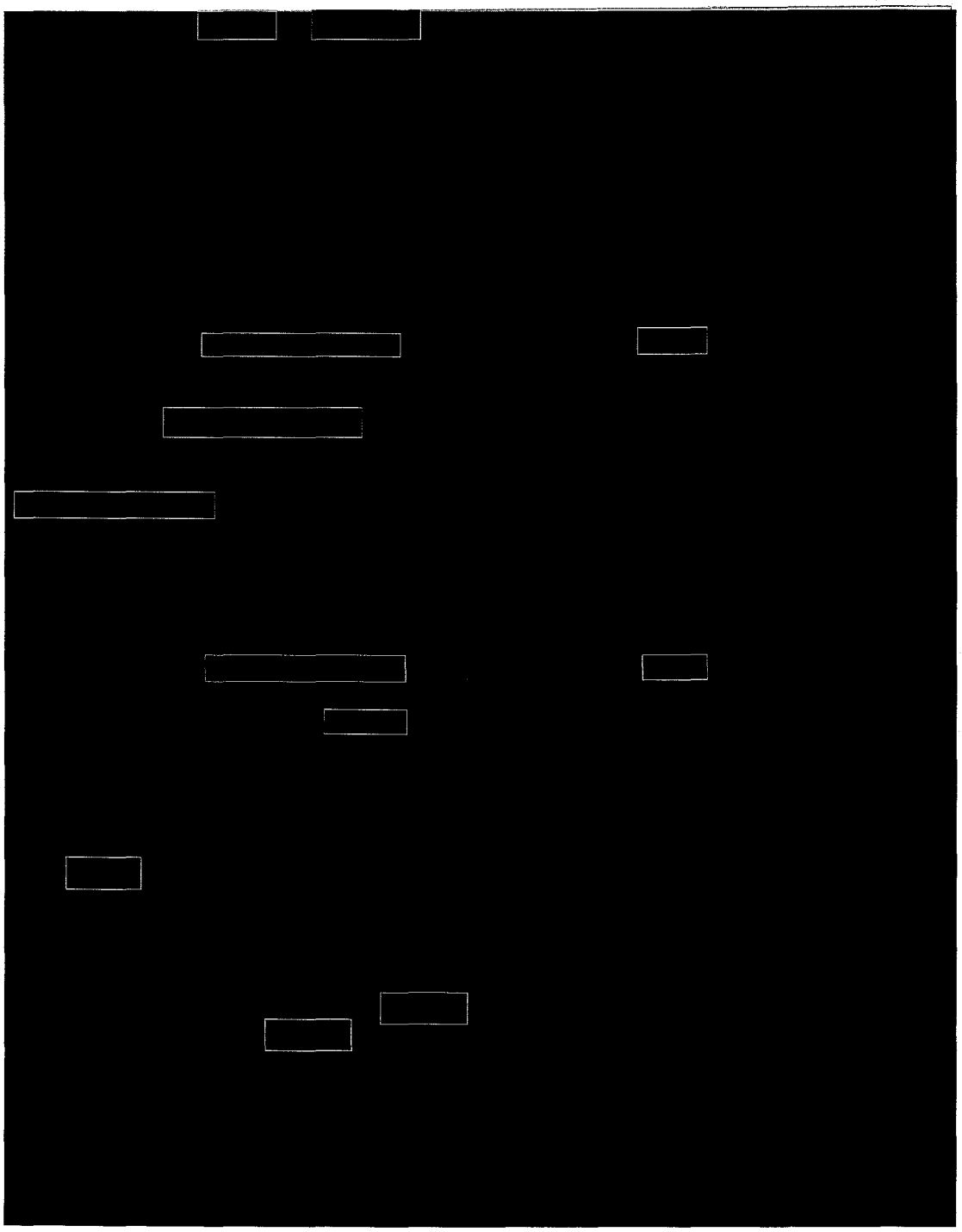
IAB Energy-DE-related briefings
2009 12 31 to 2015 07 30

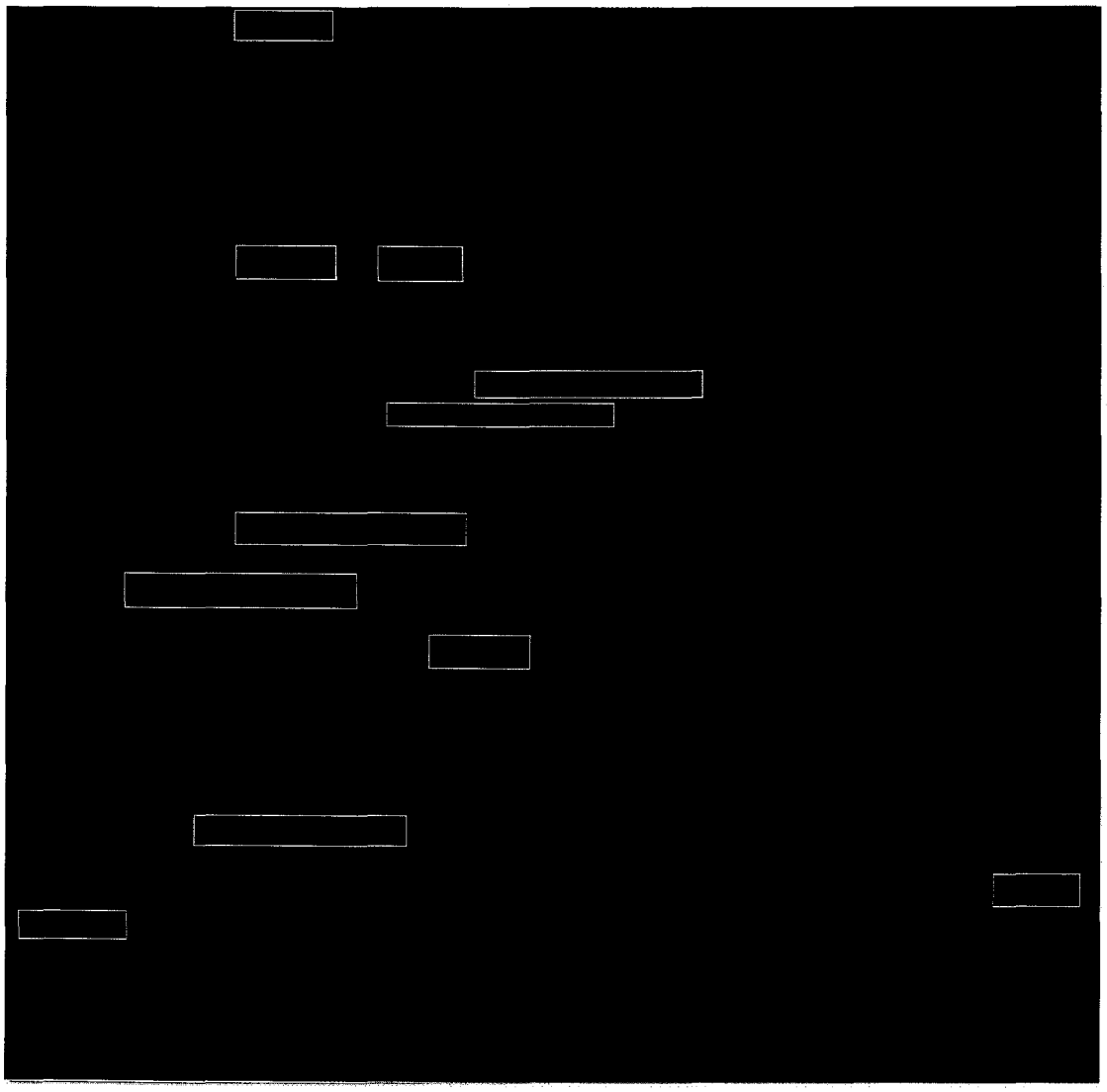
[redacted]

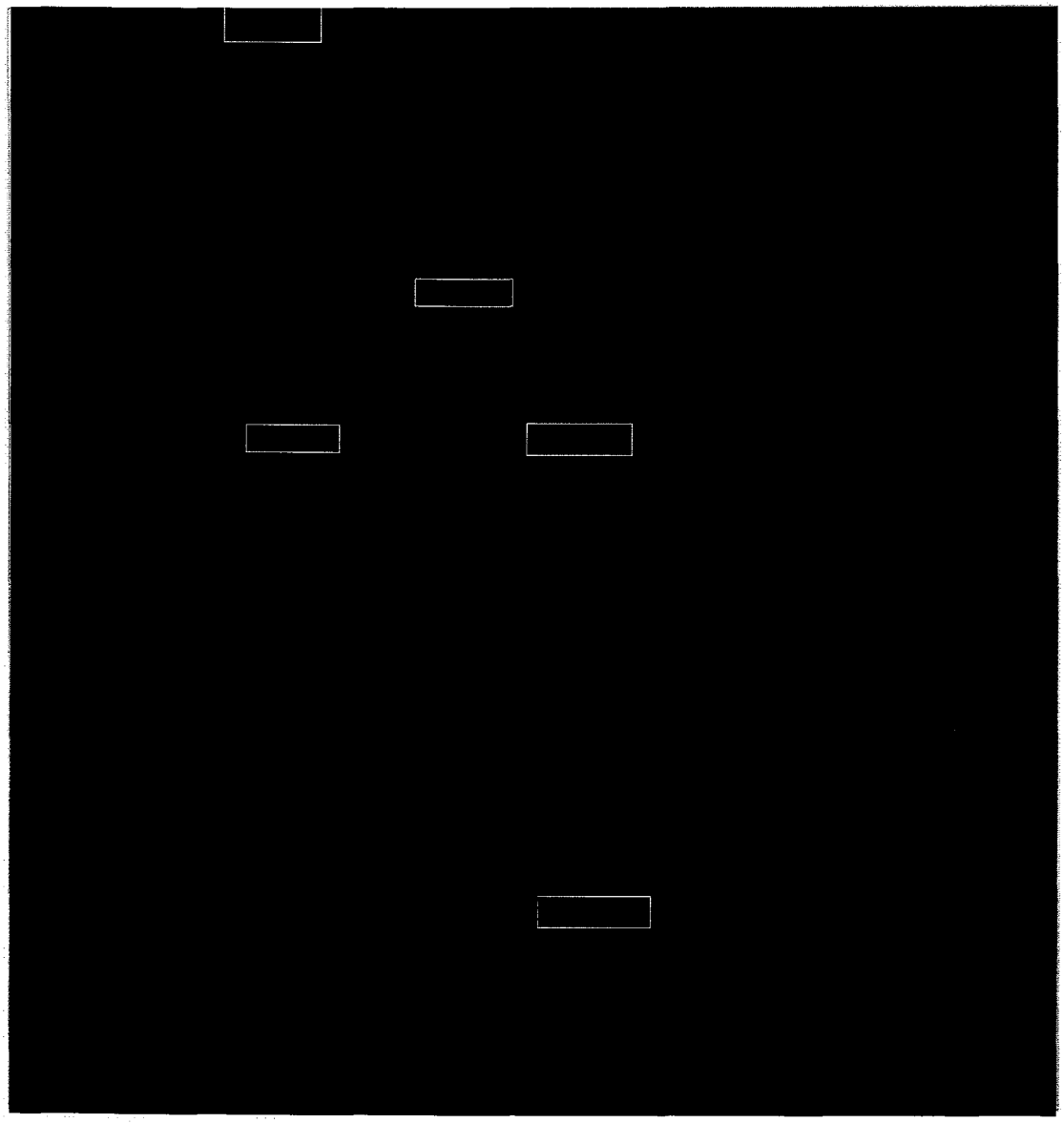


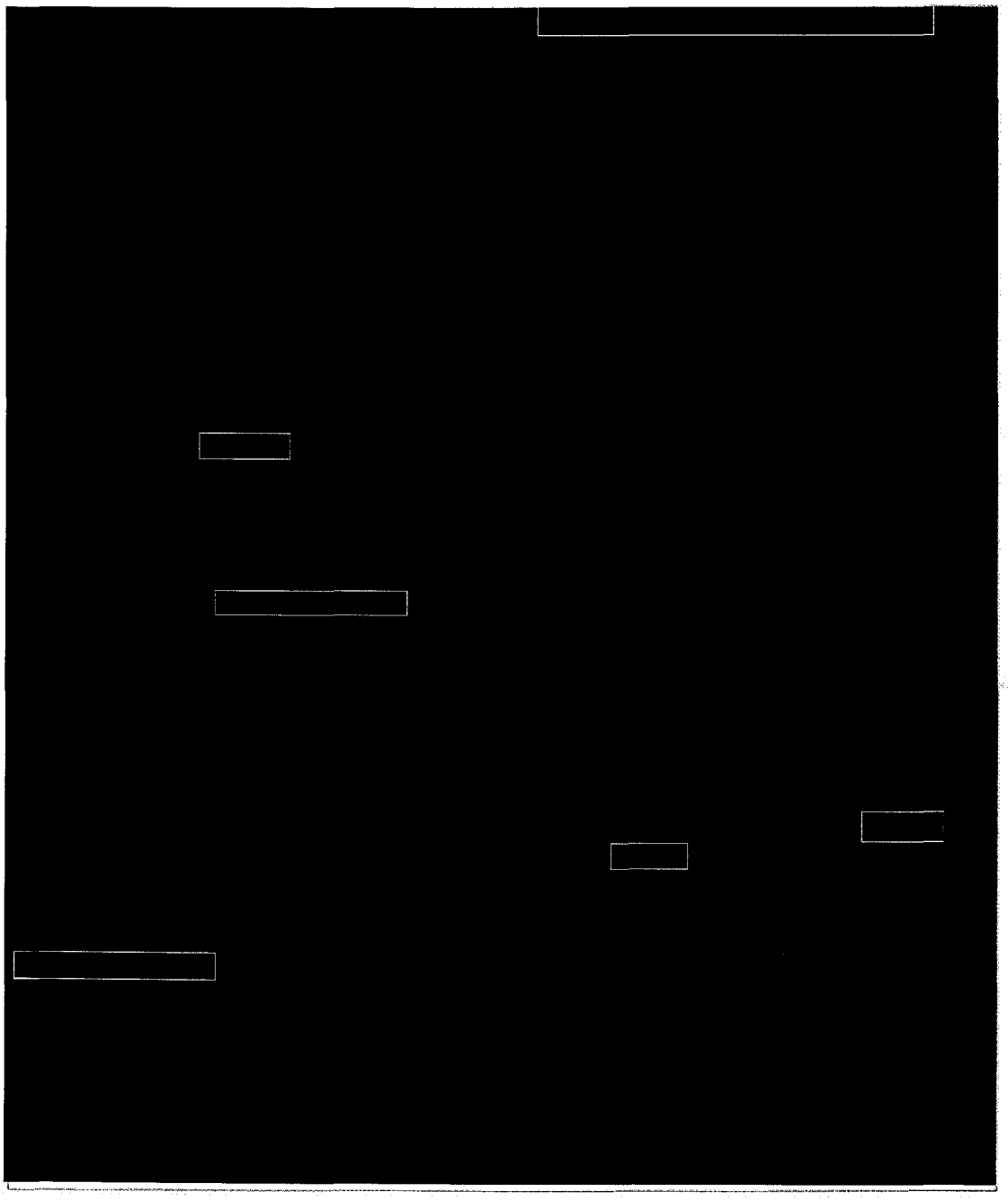


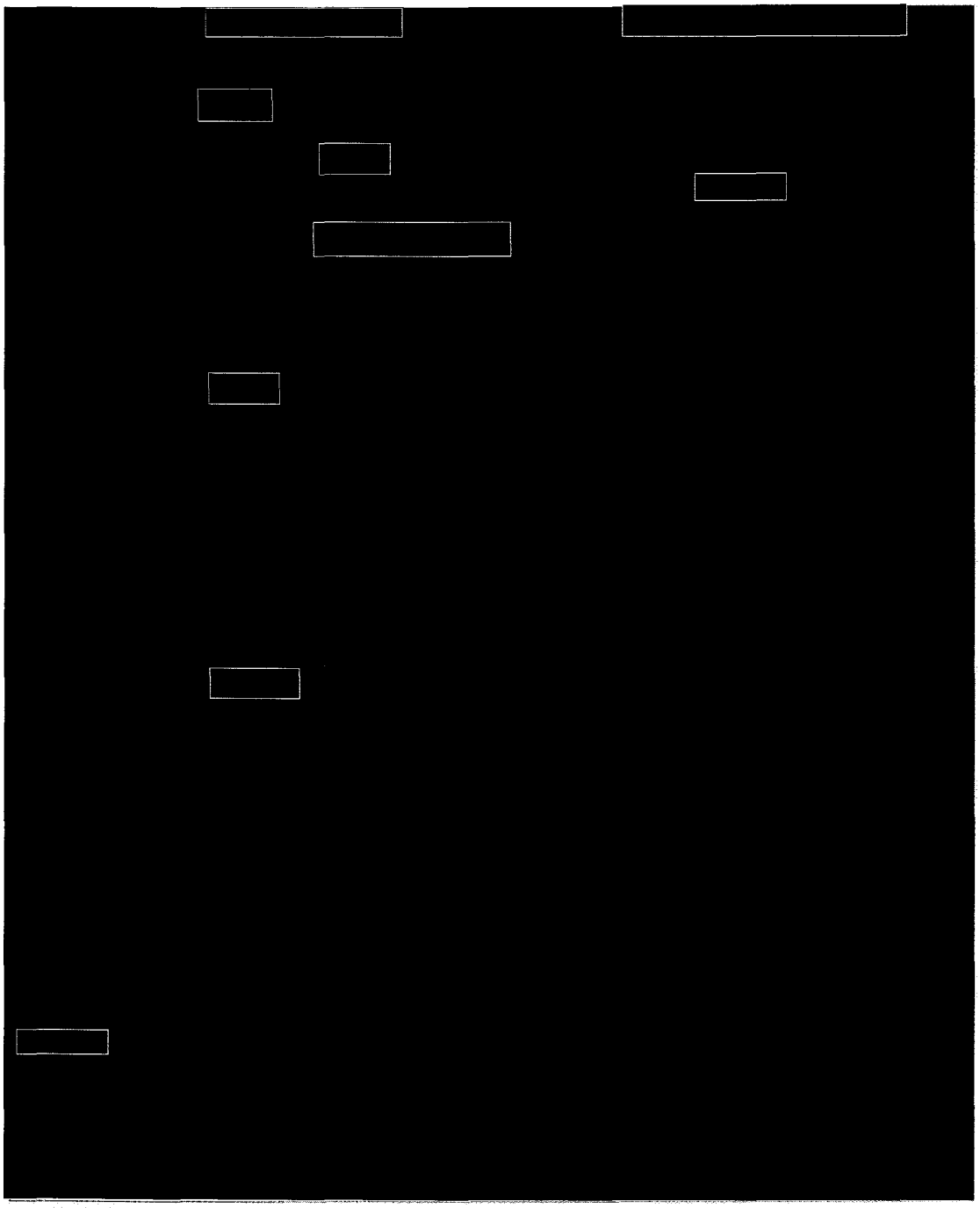
[redacted]

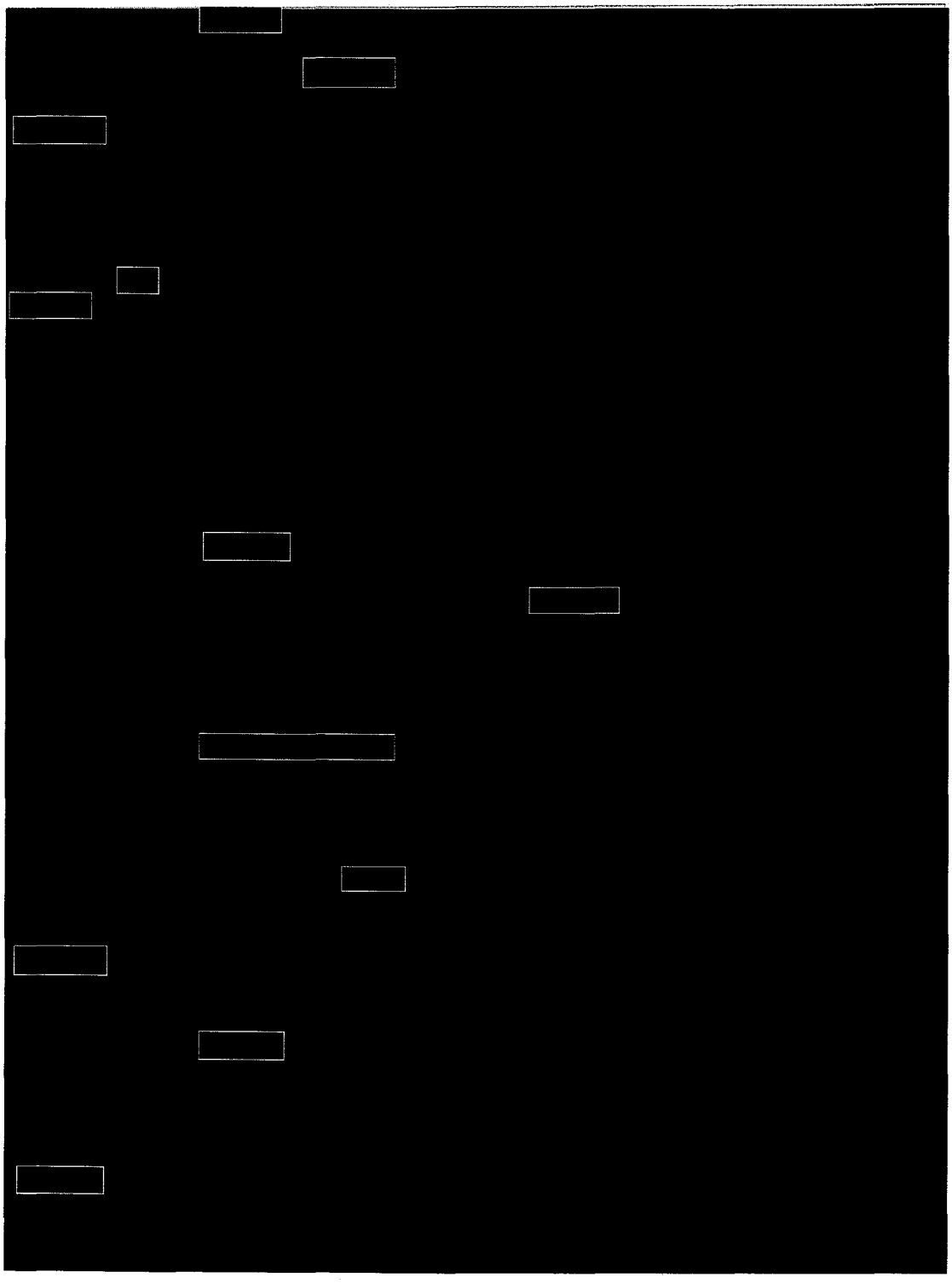


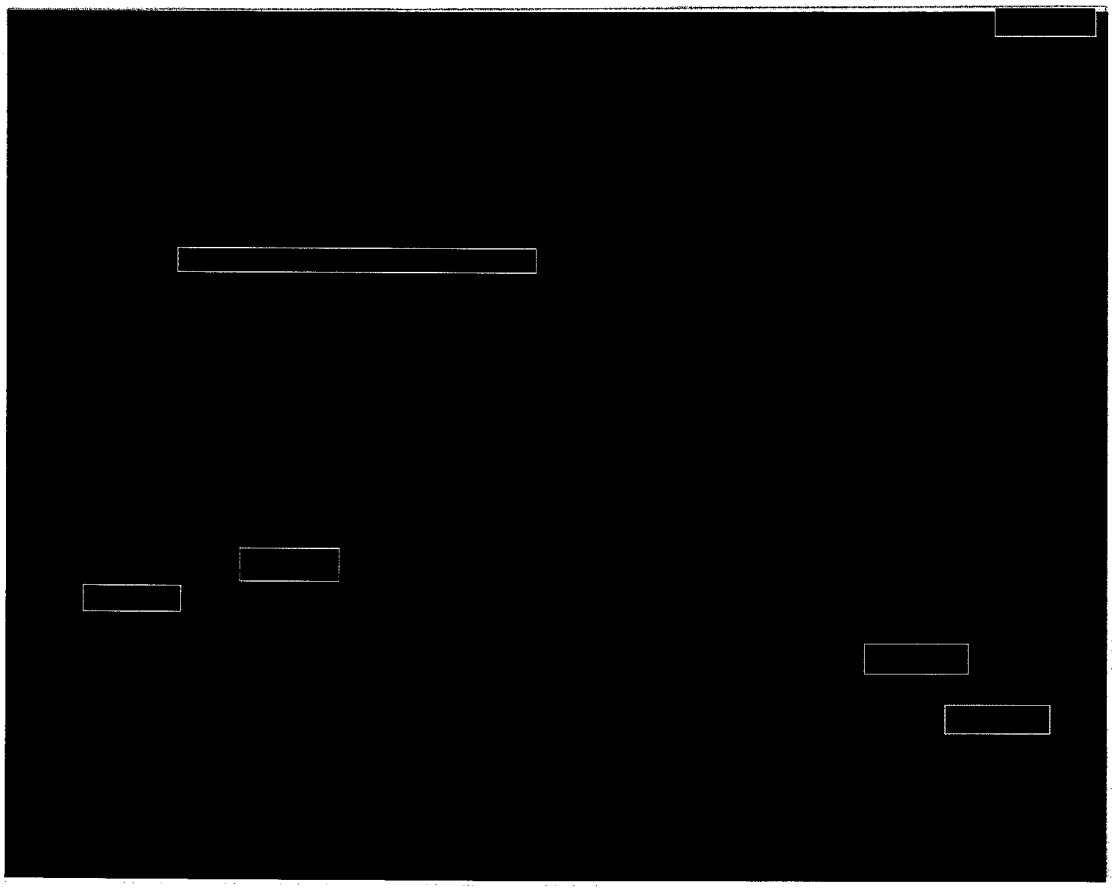




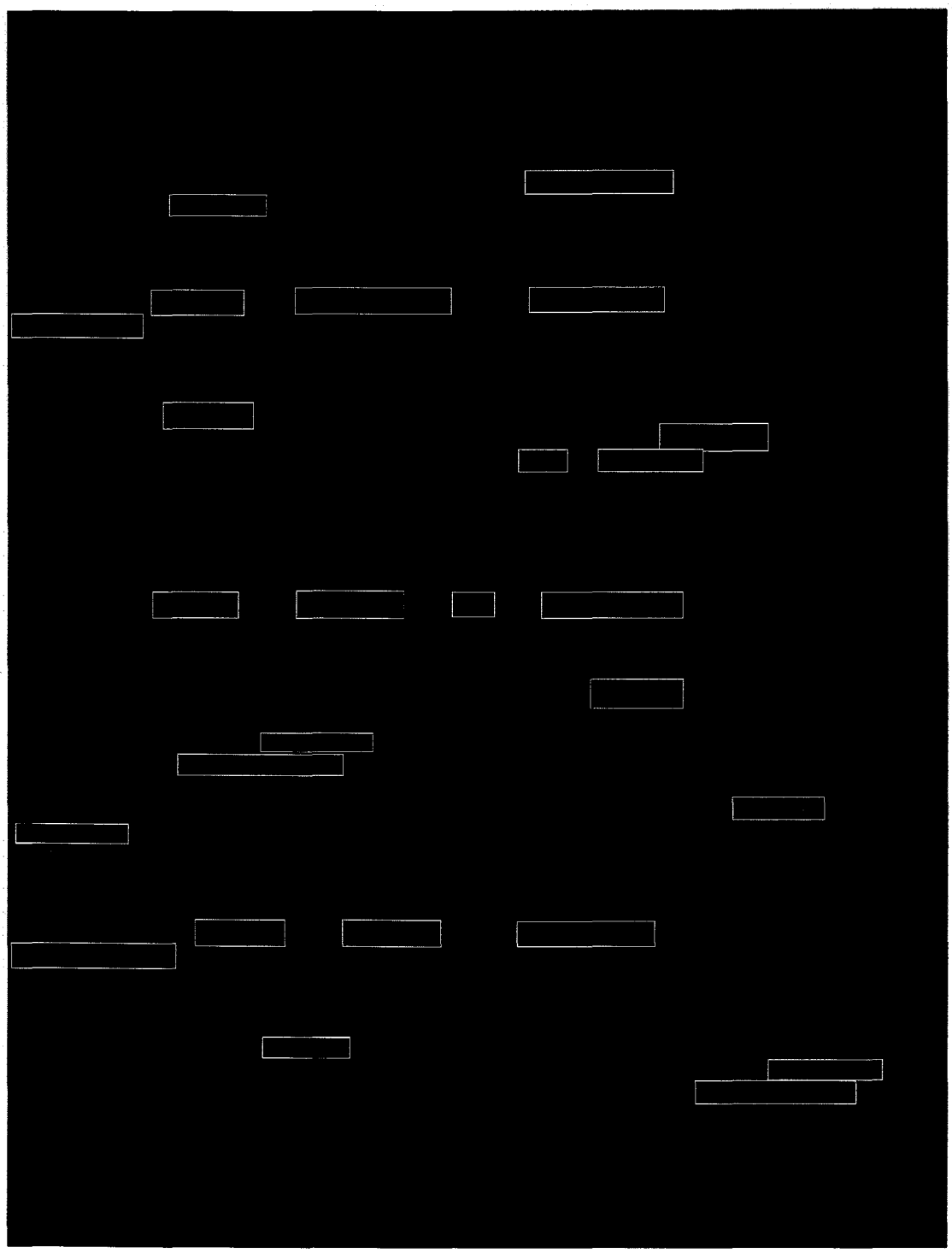


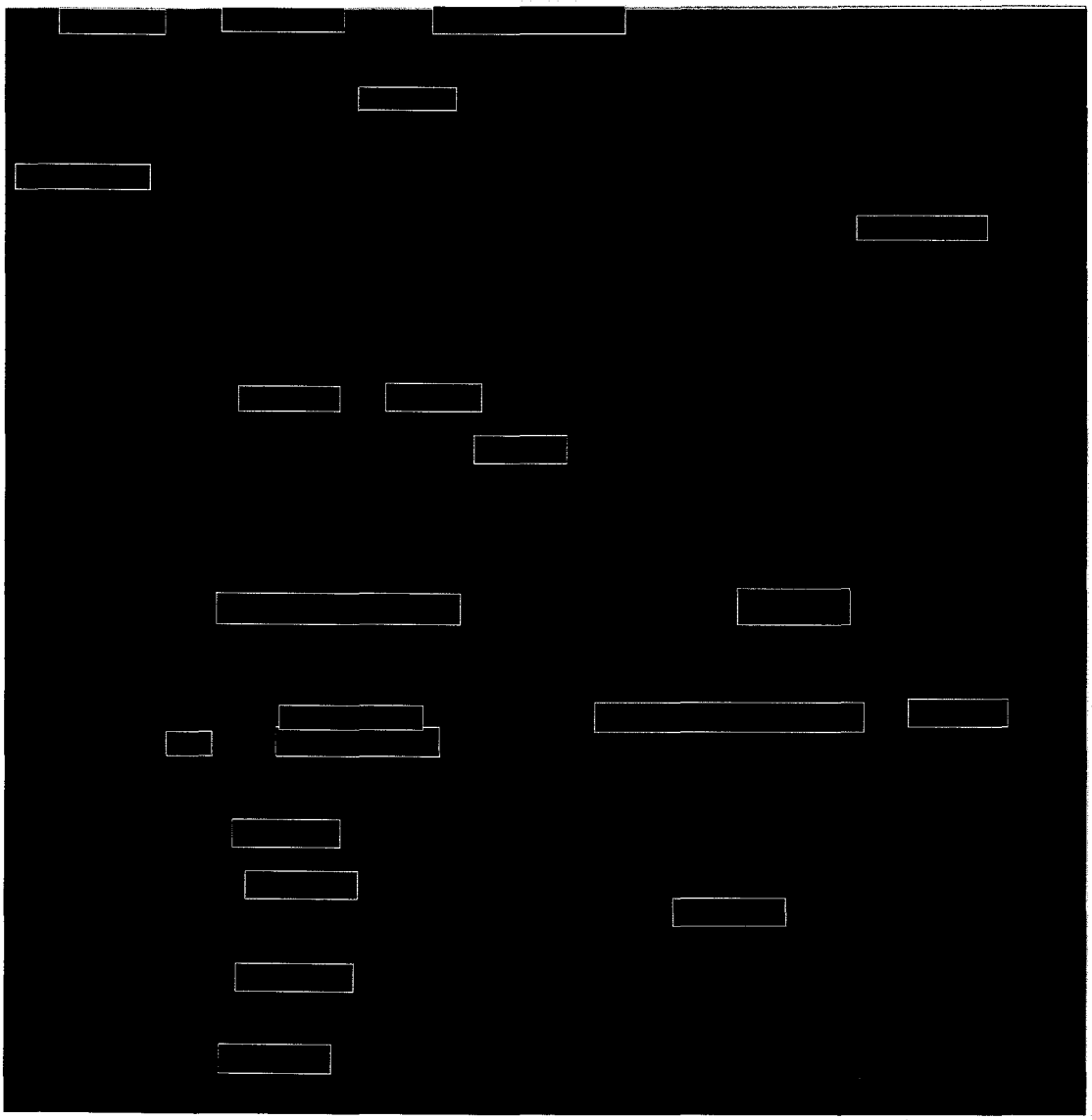


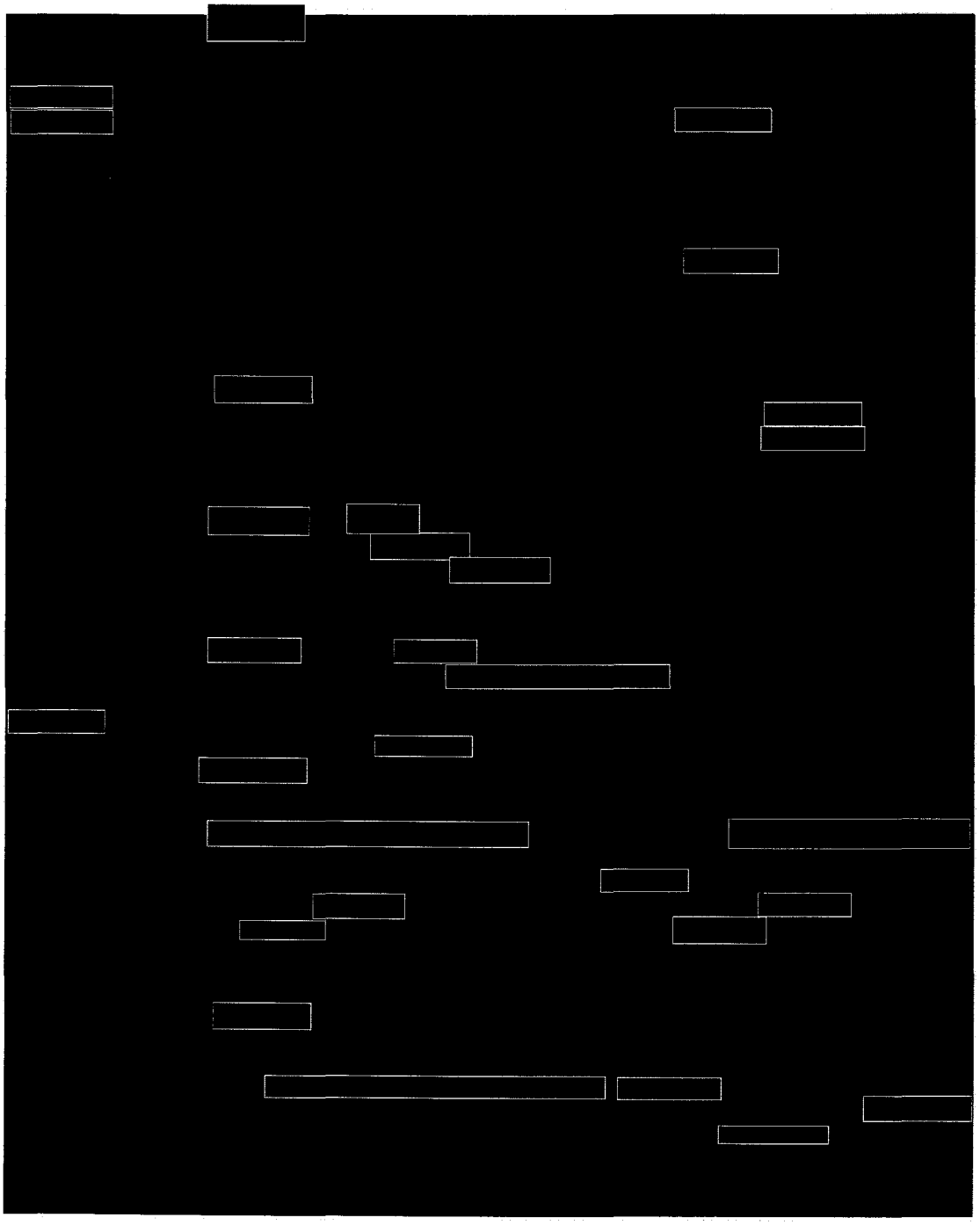


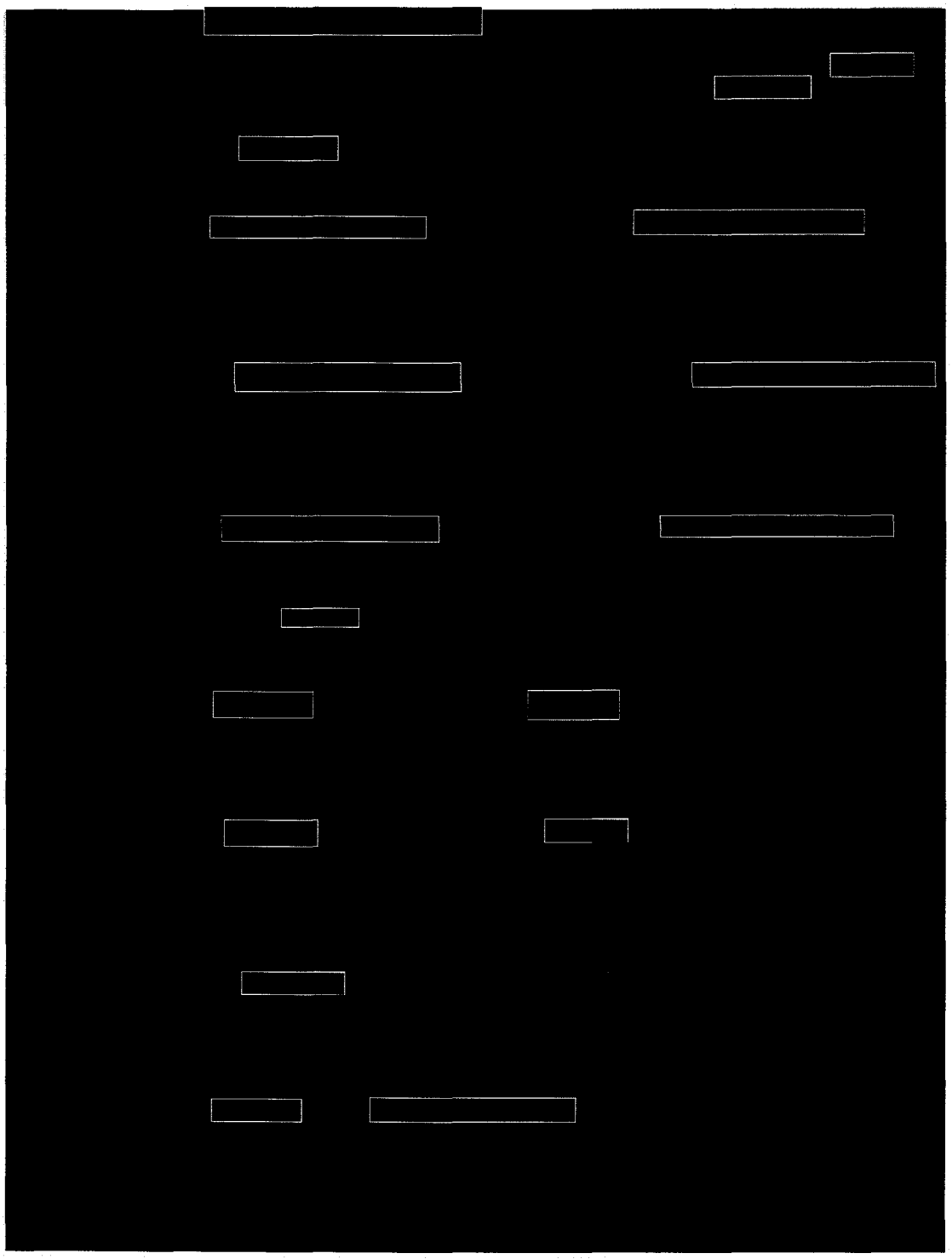


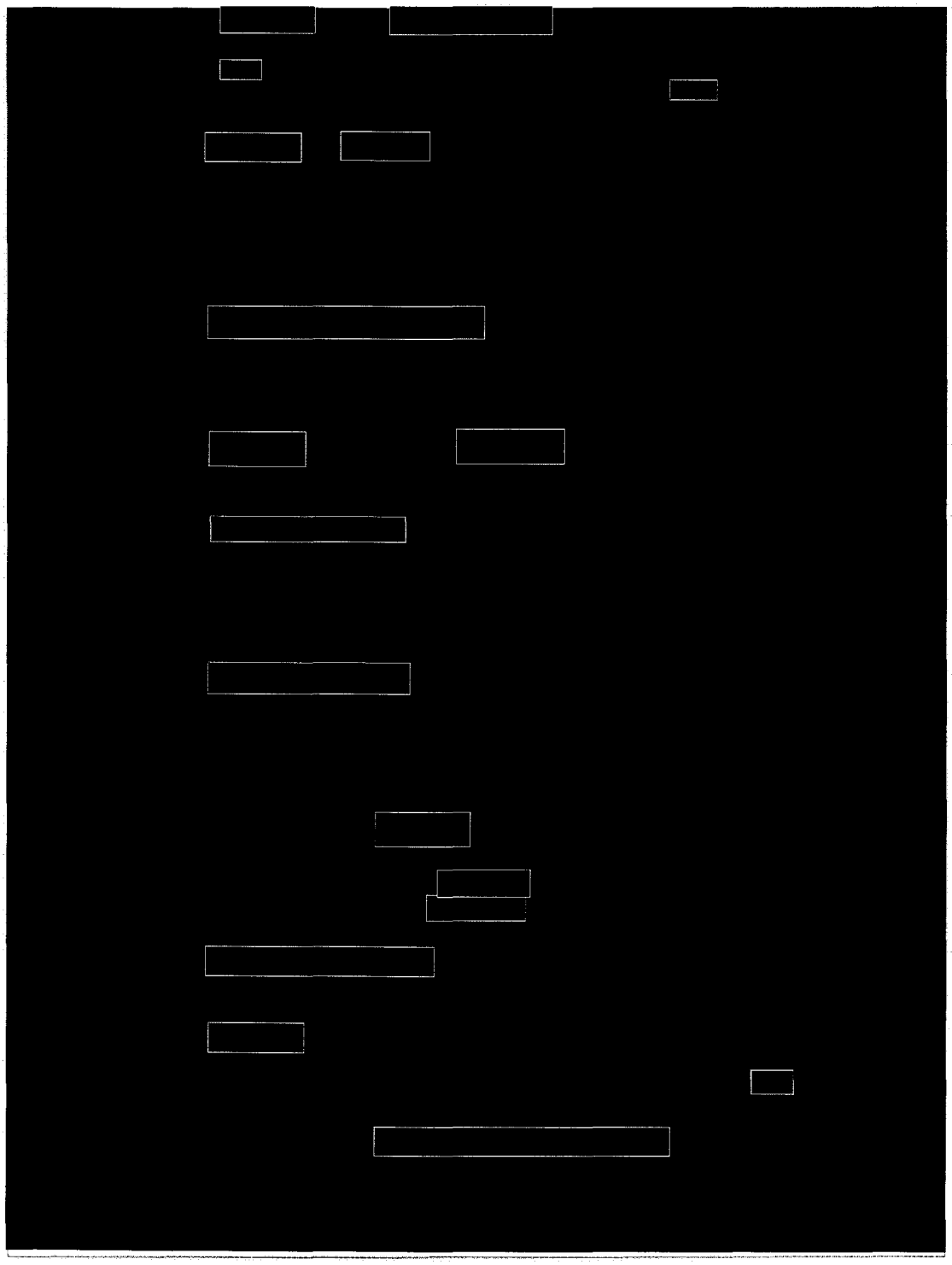
[redacted]	
Description	



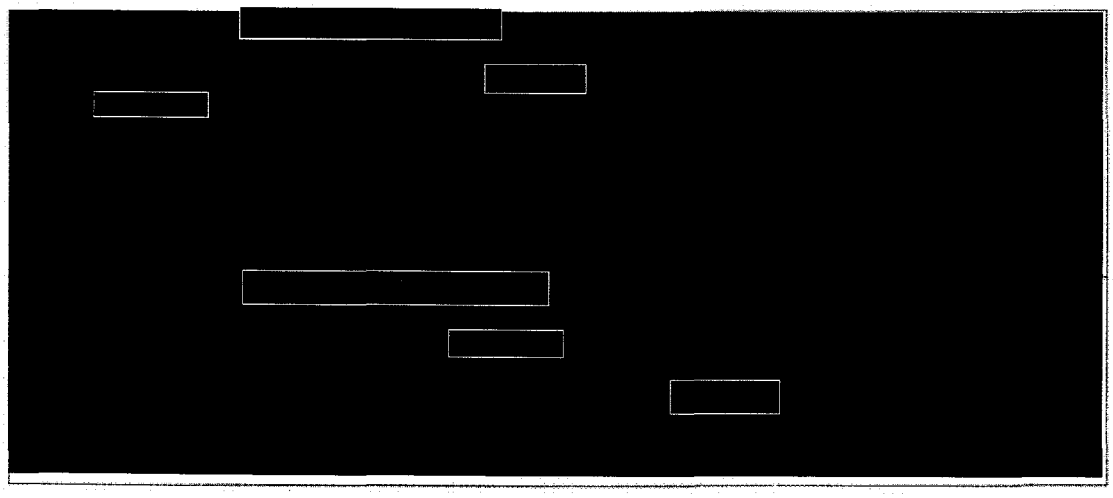






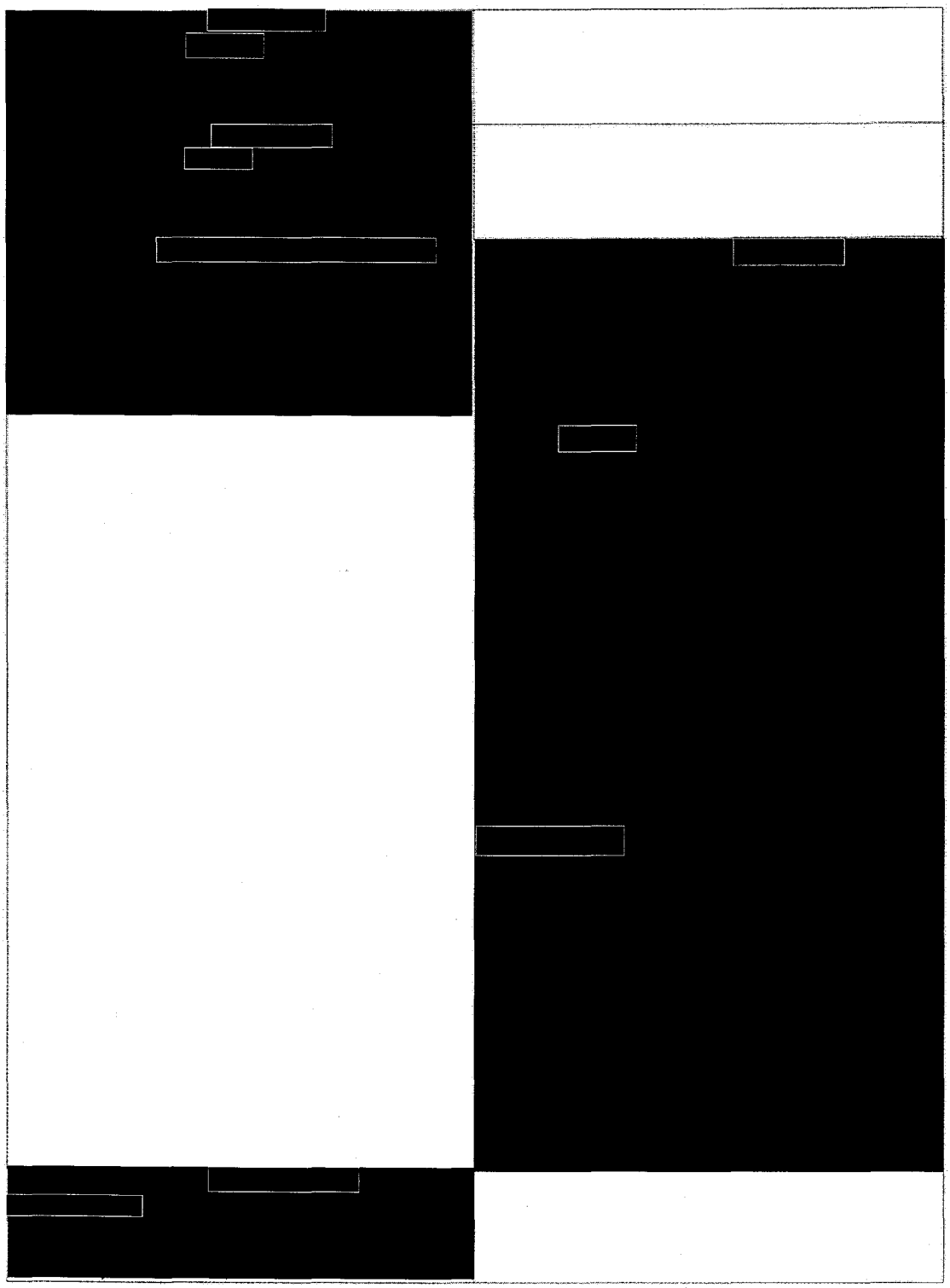


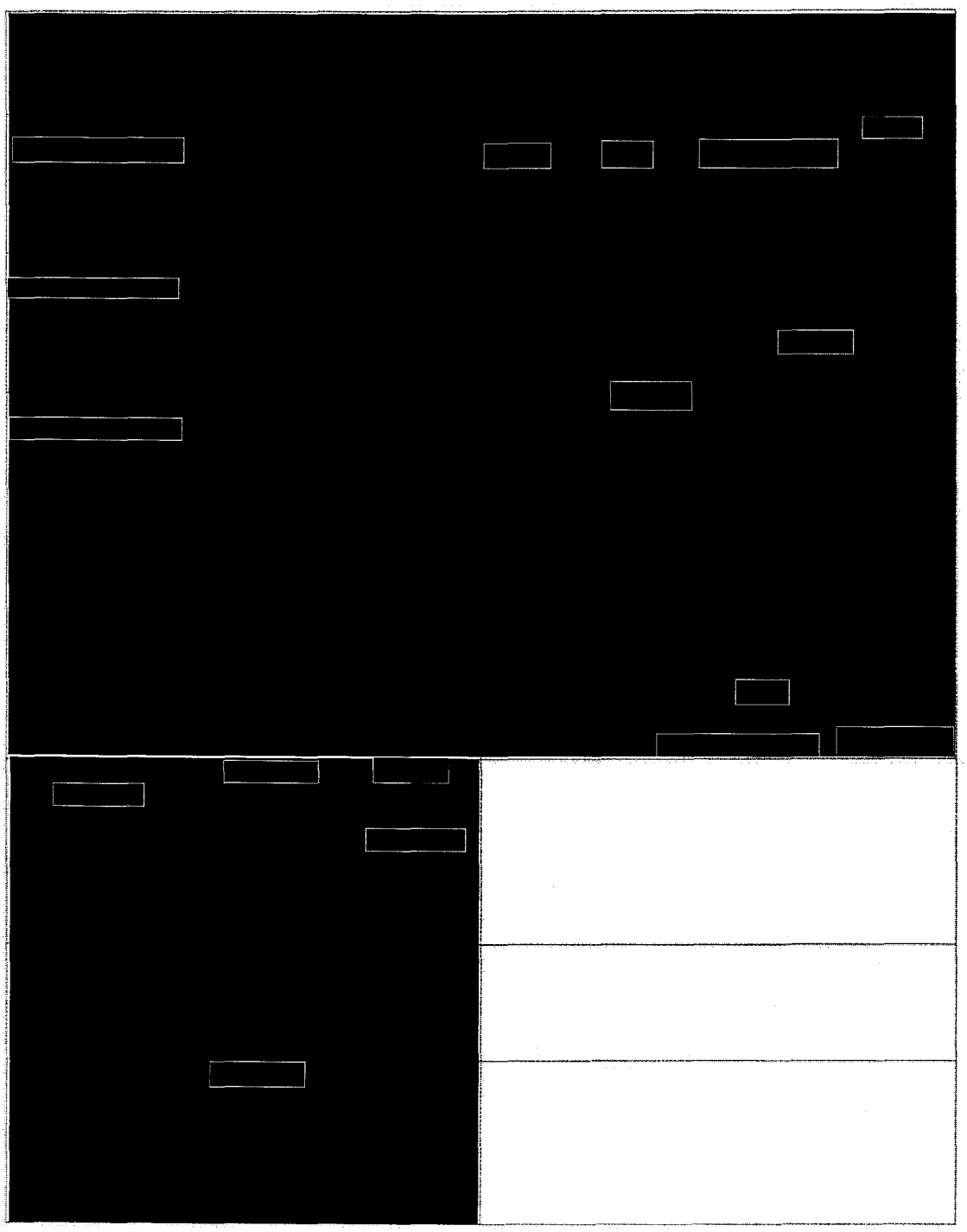
[redacted]

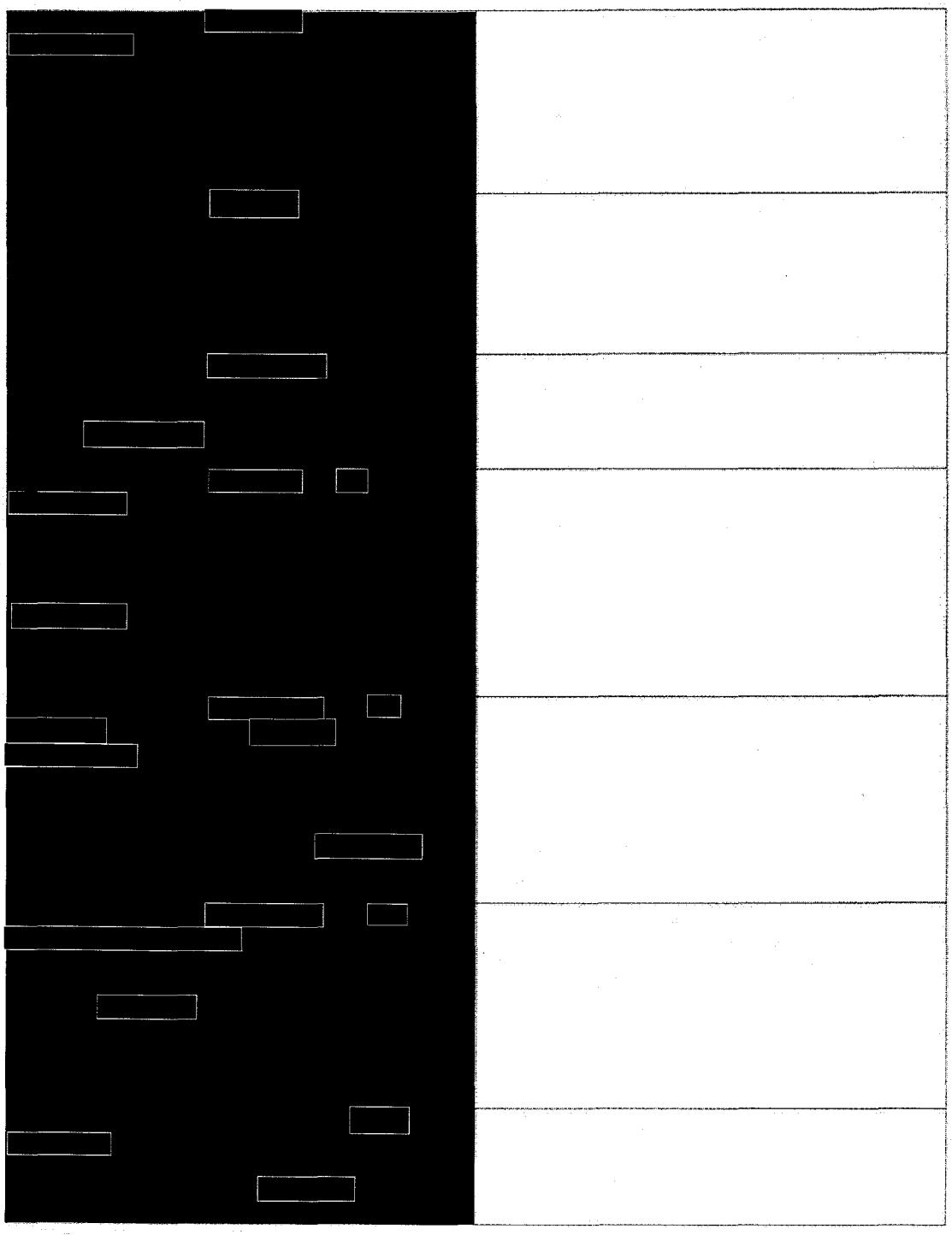


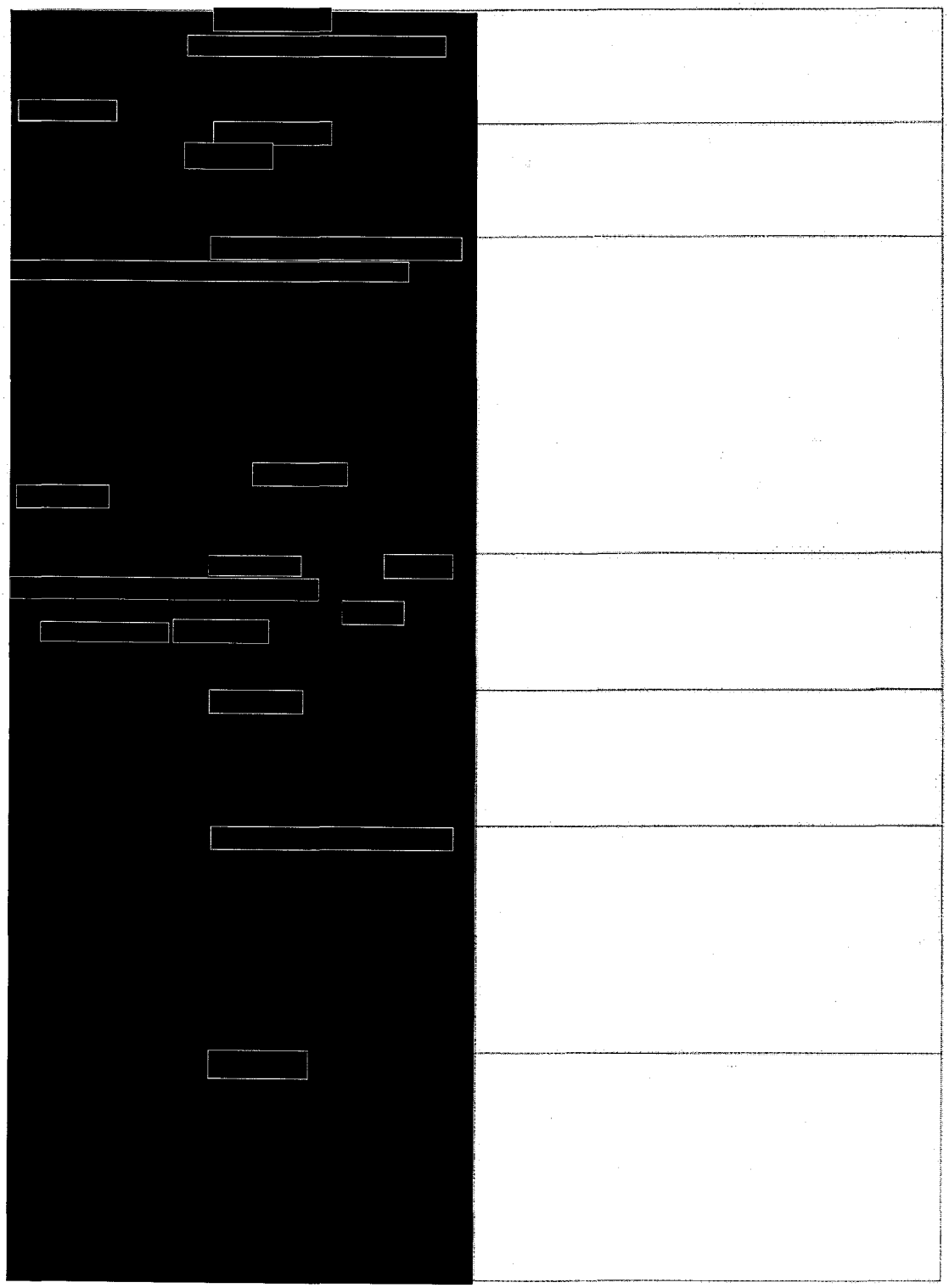
[redacted]

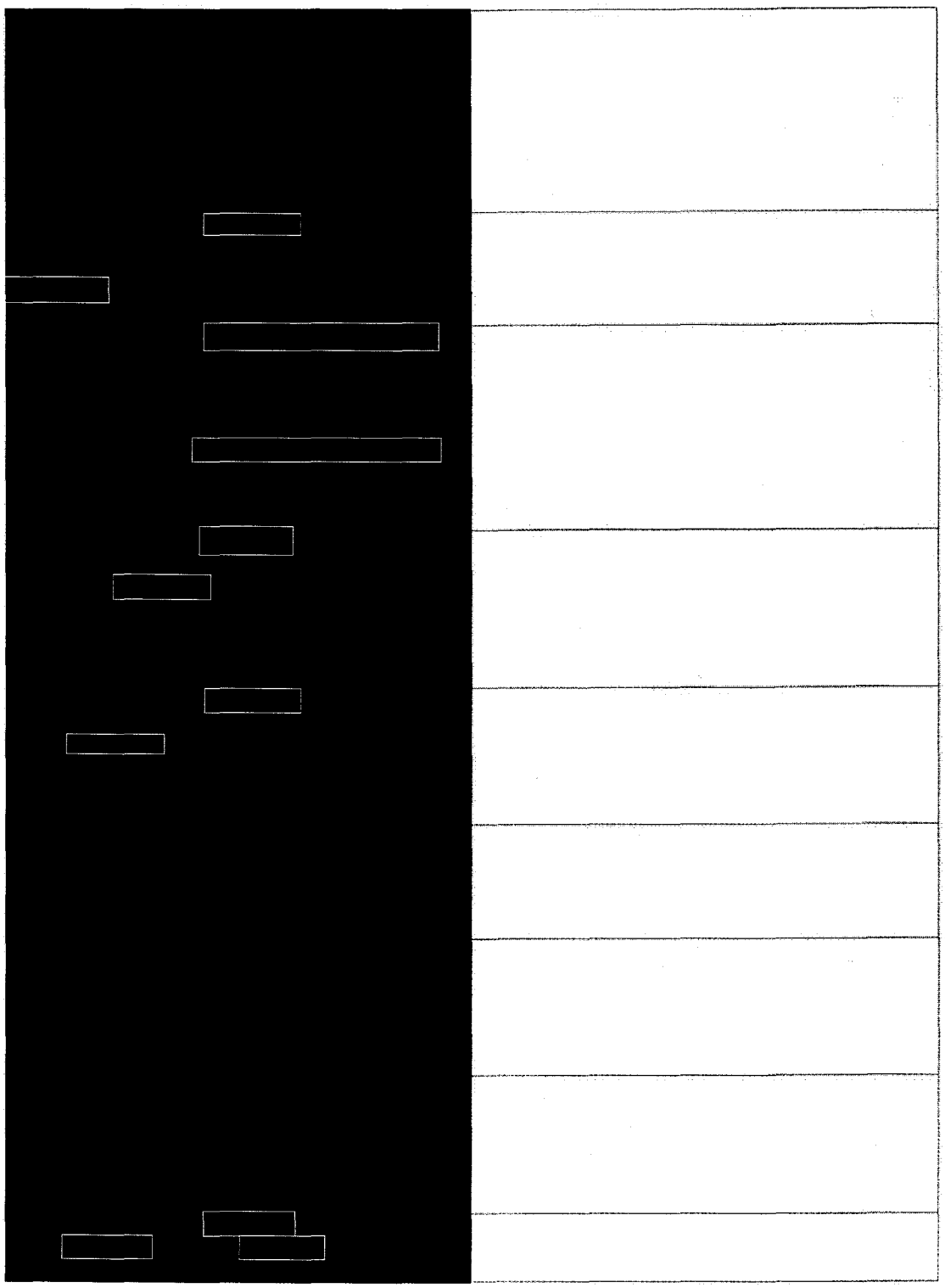
Description	Feedback
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	

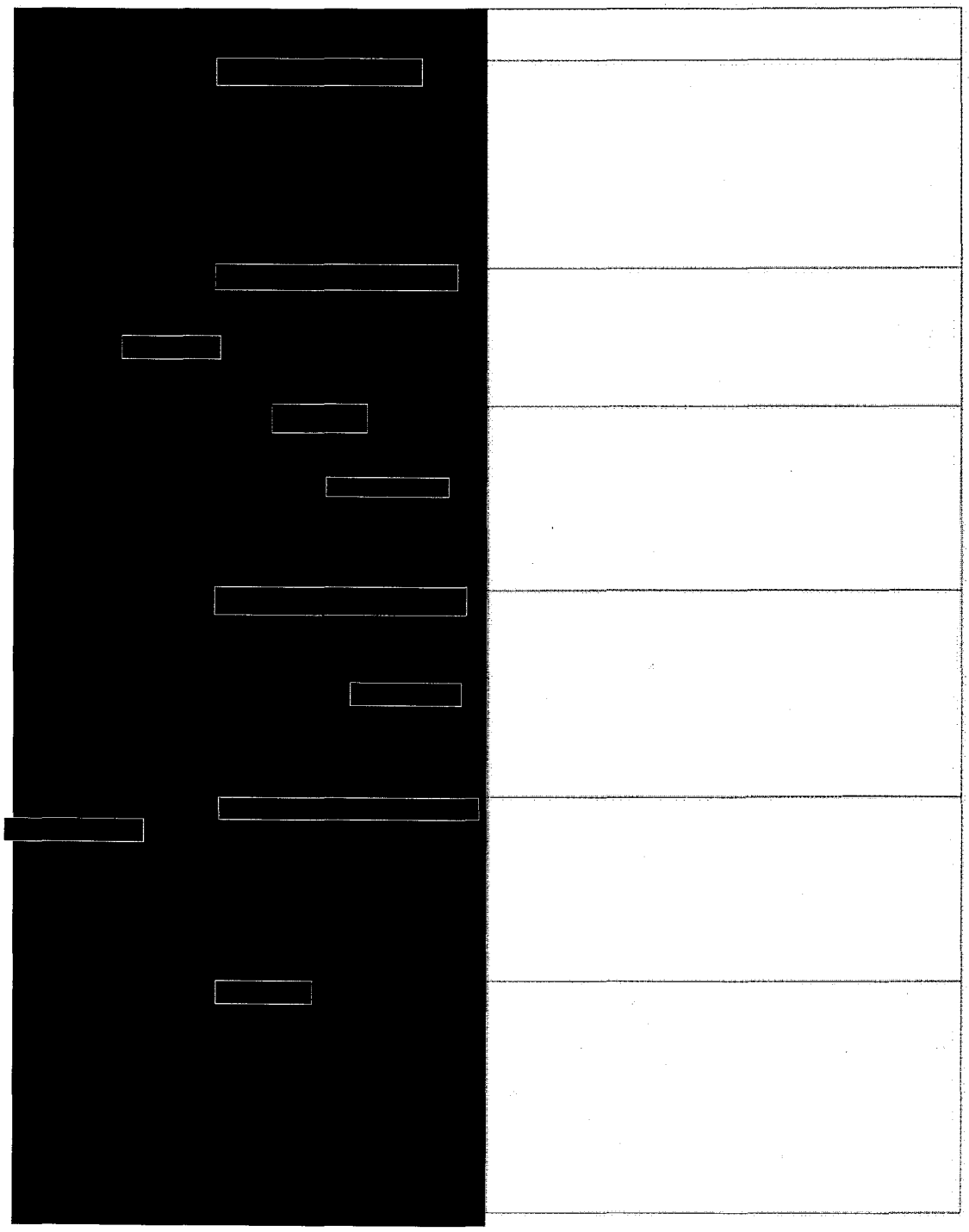


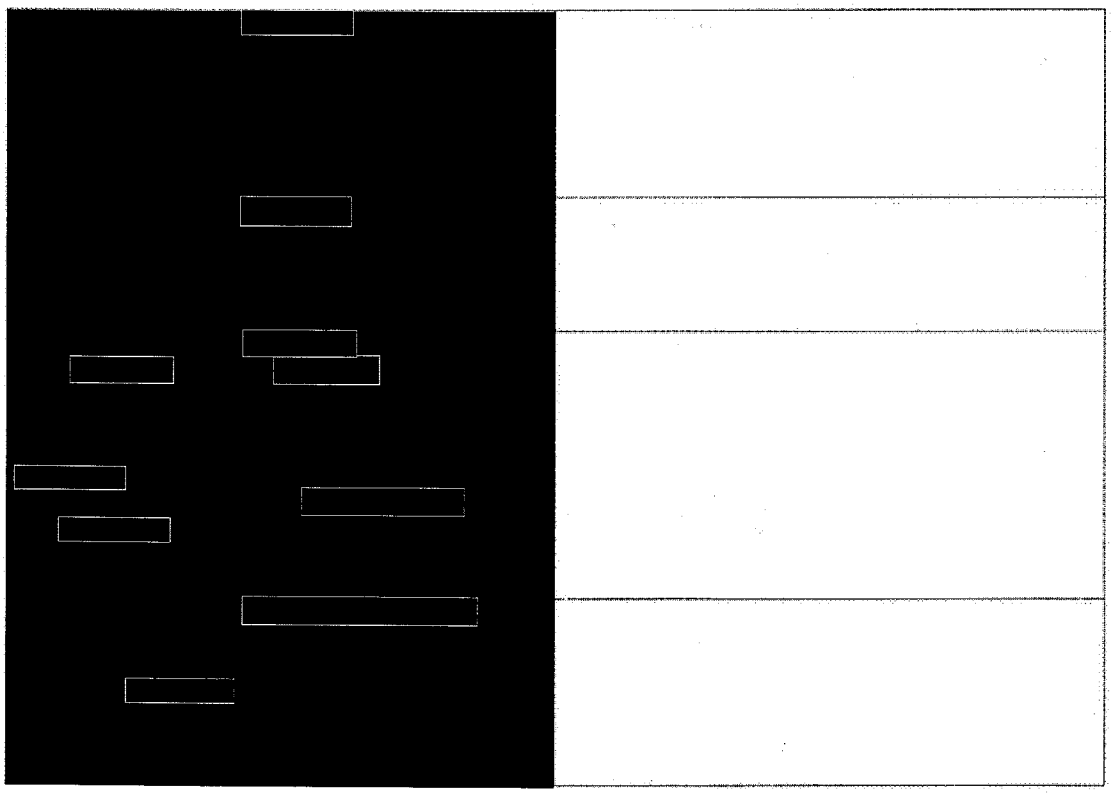


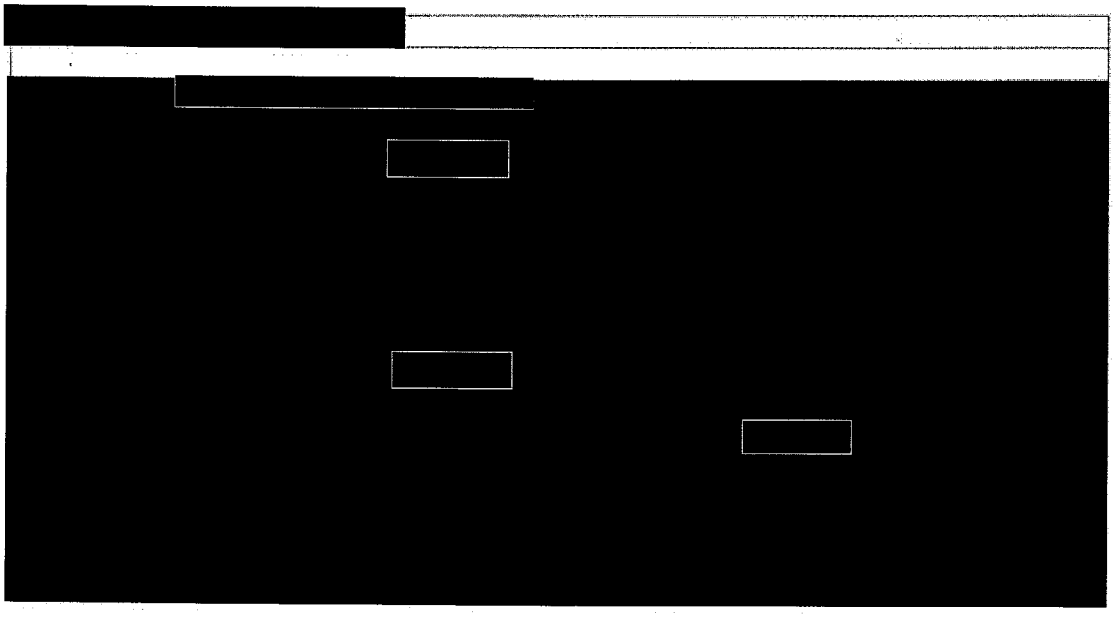


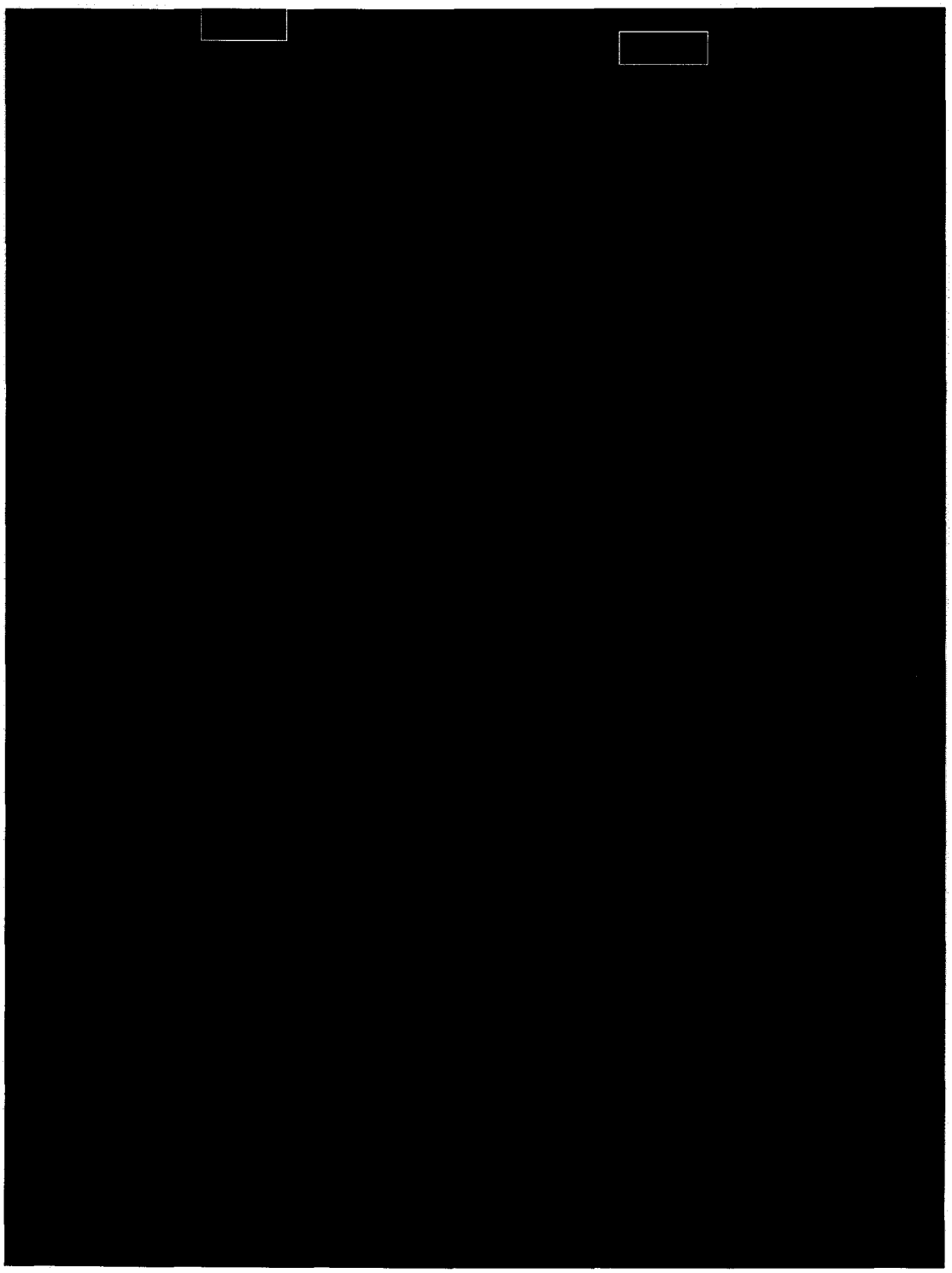


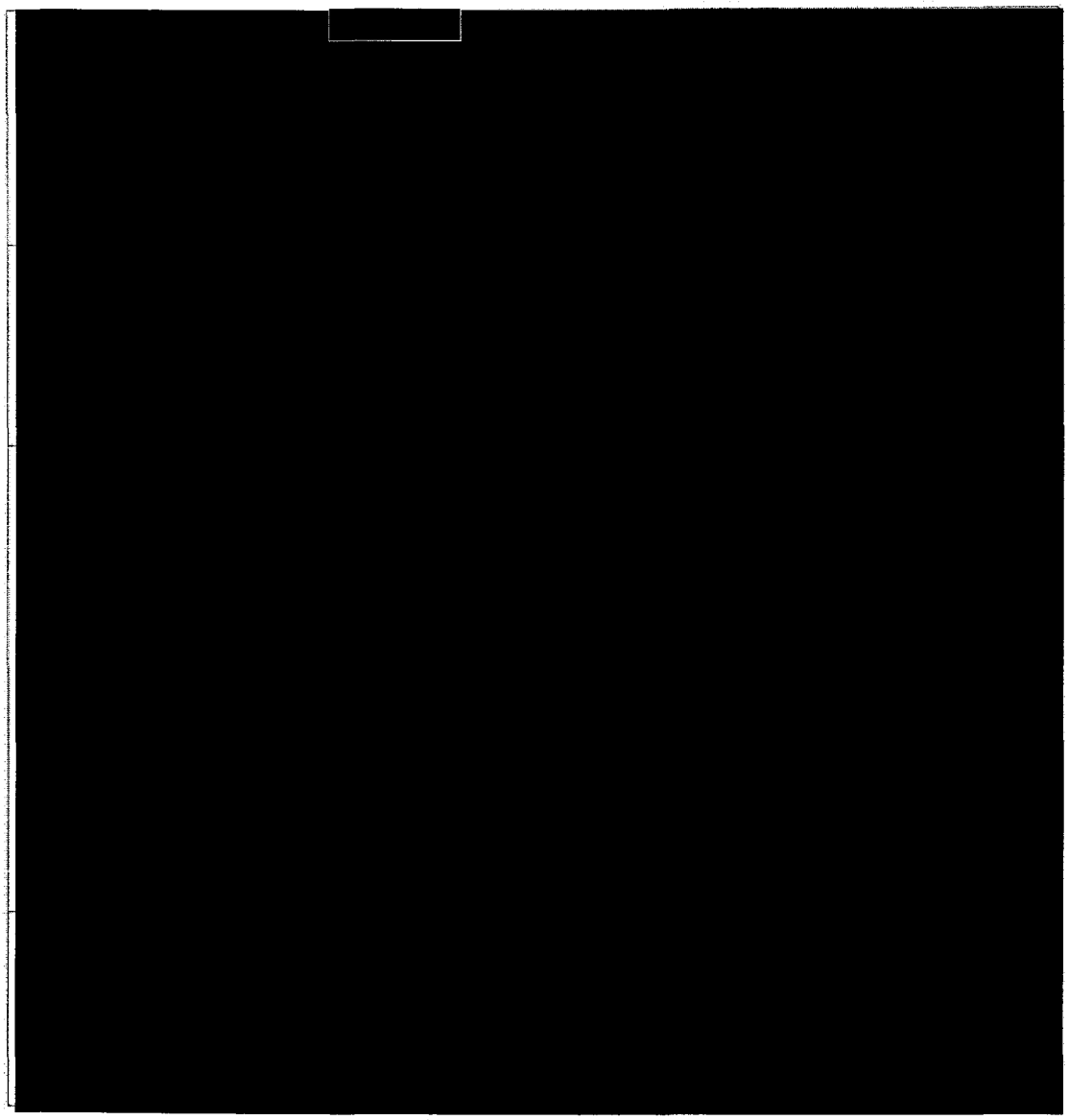


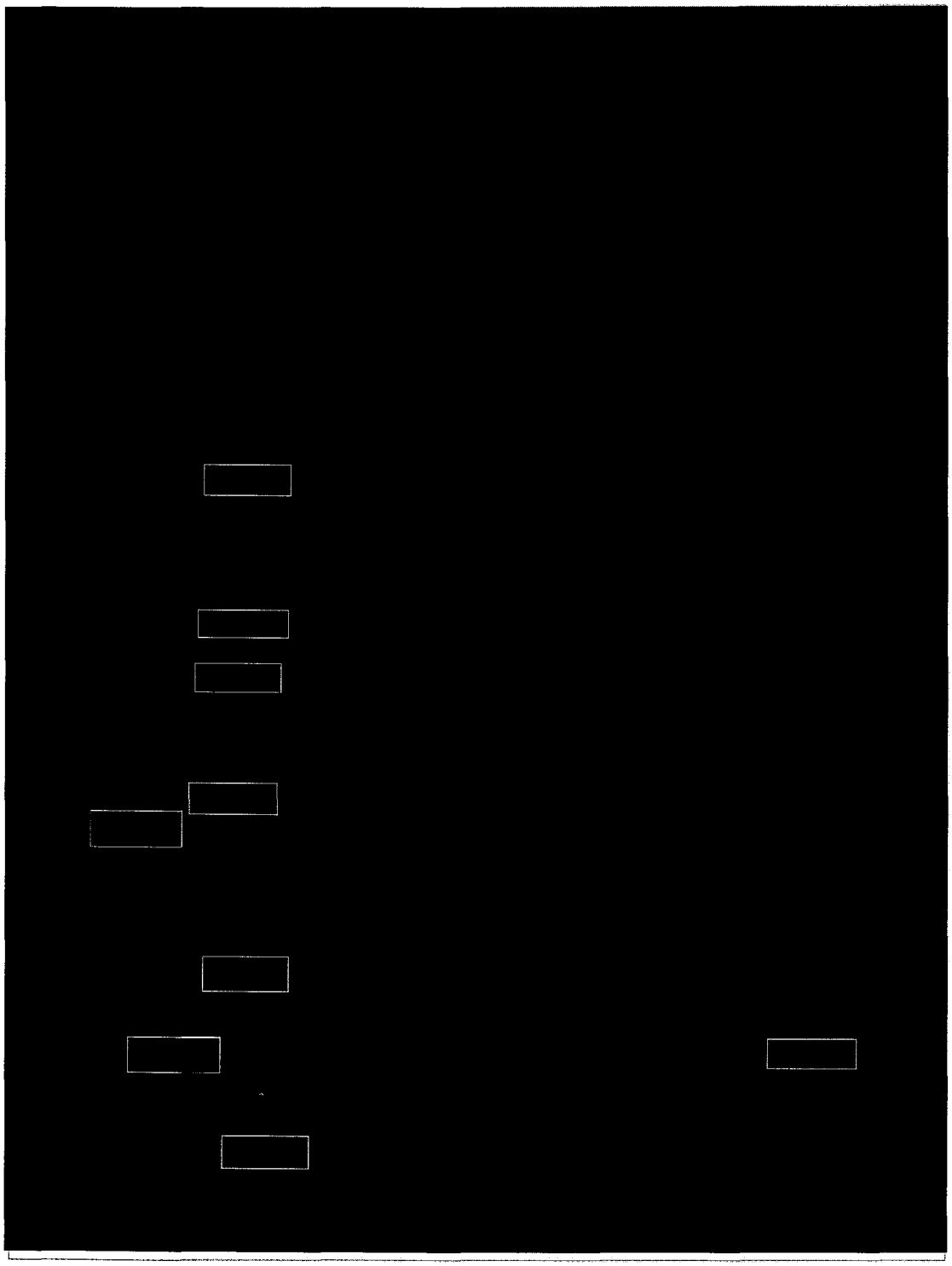


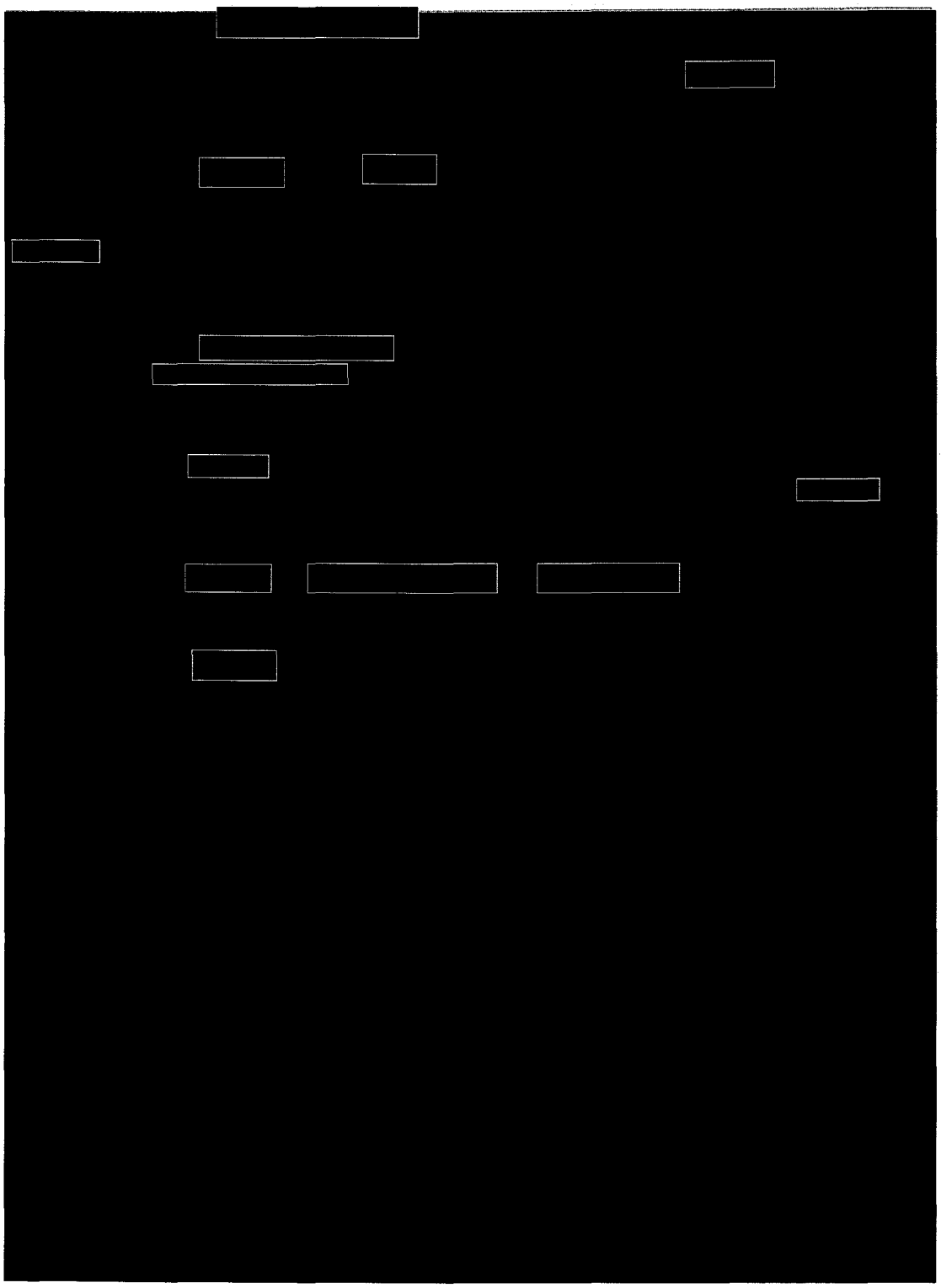


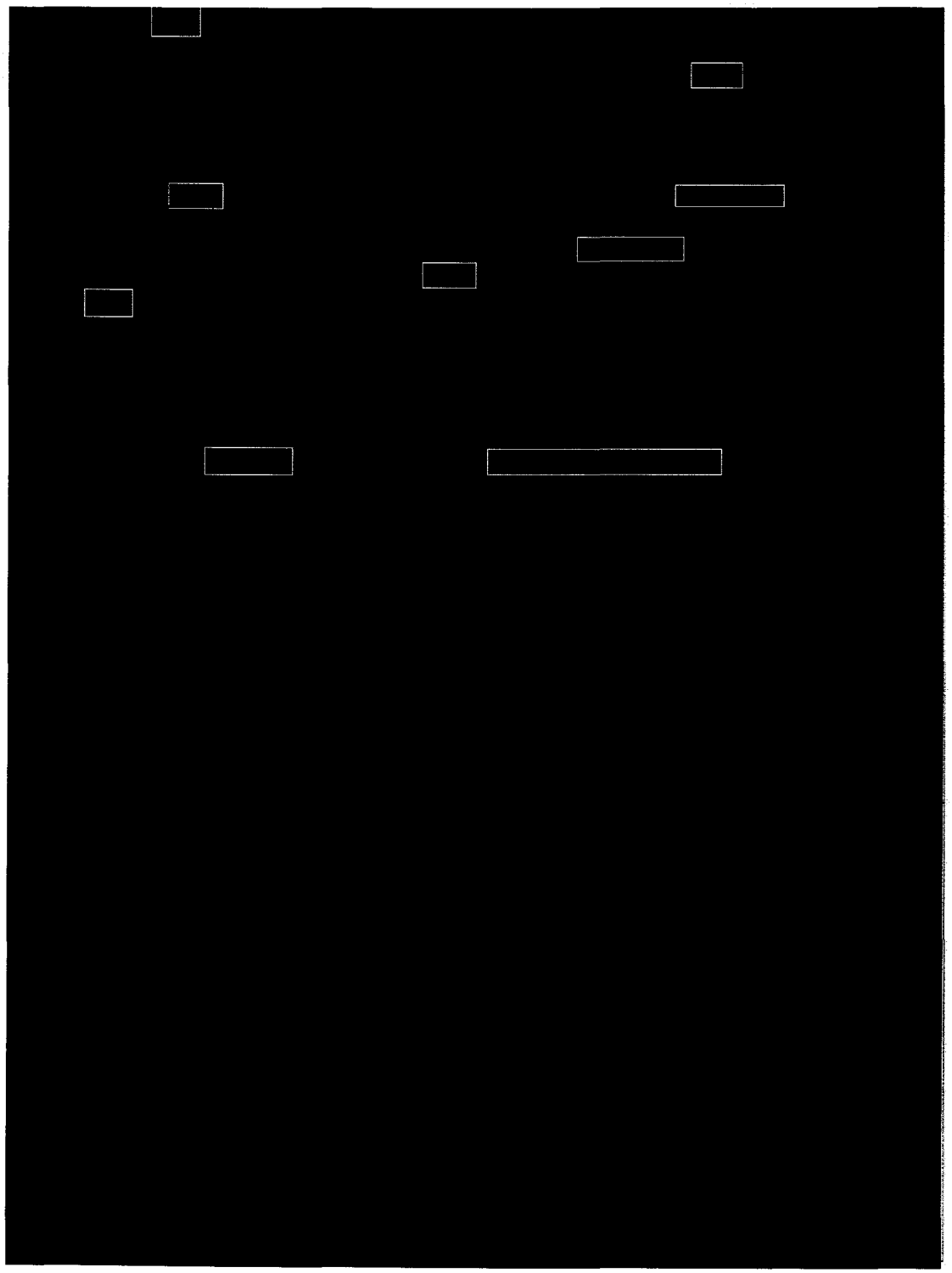


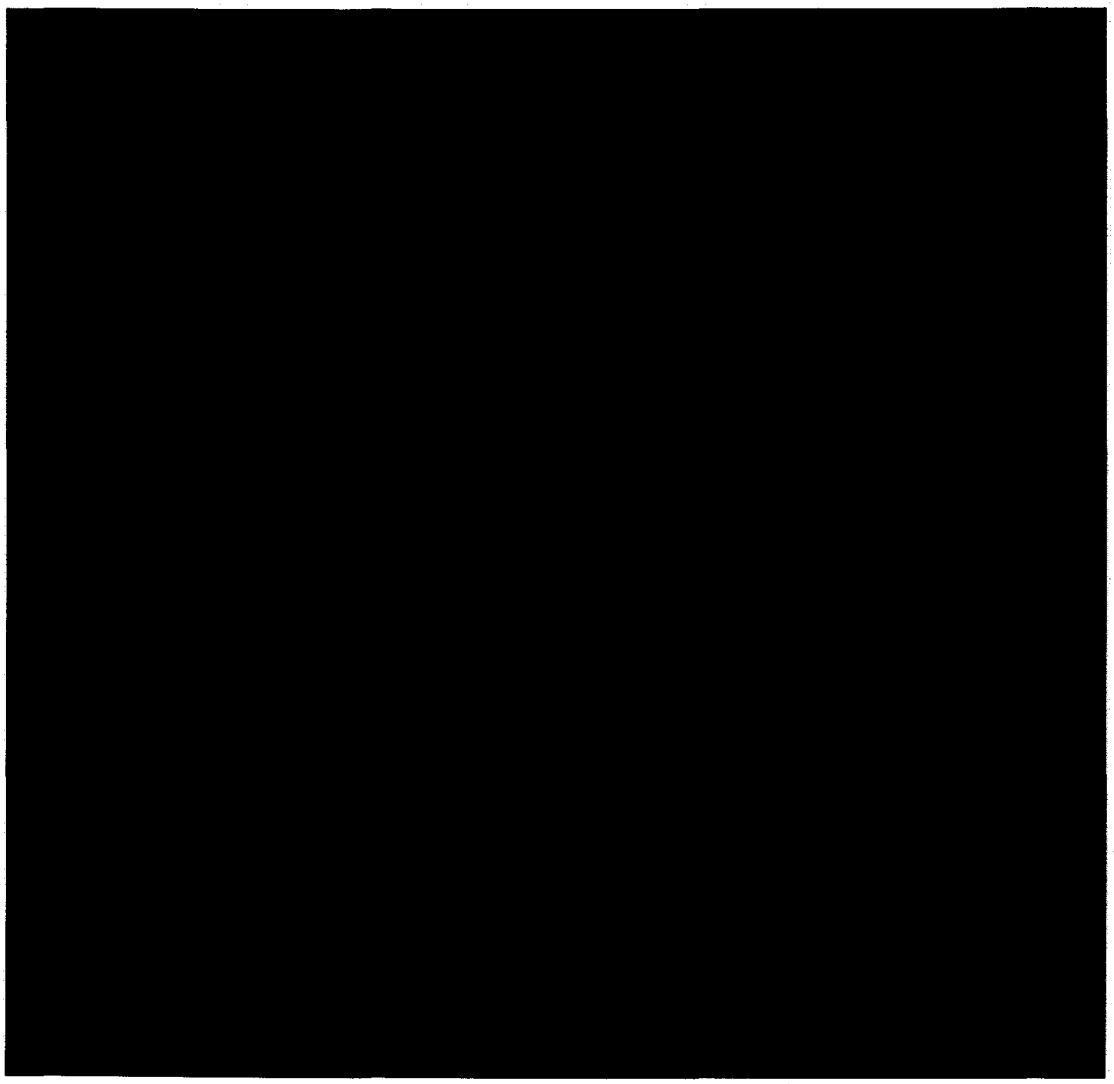


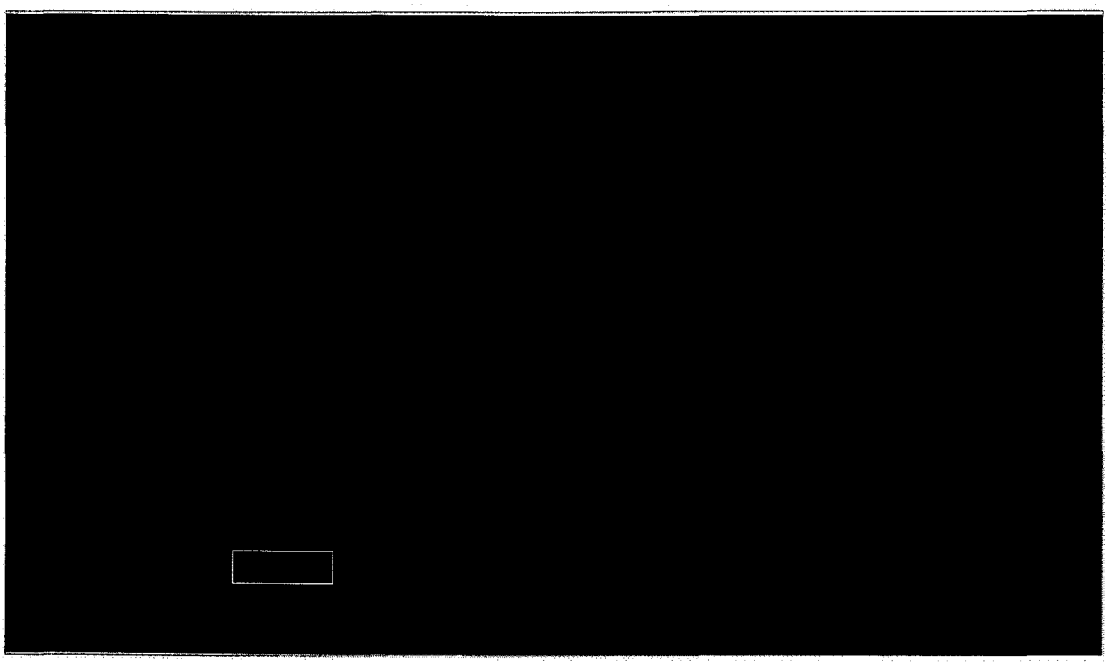


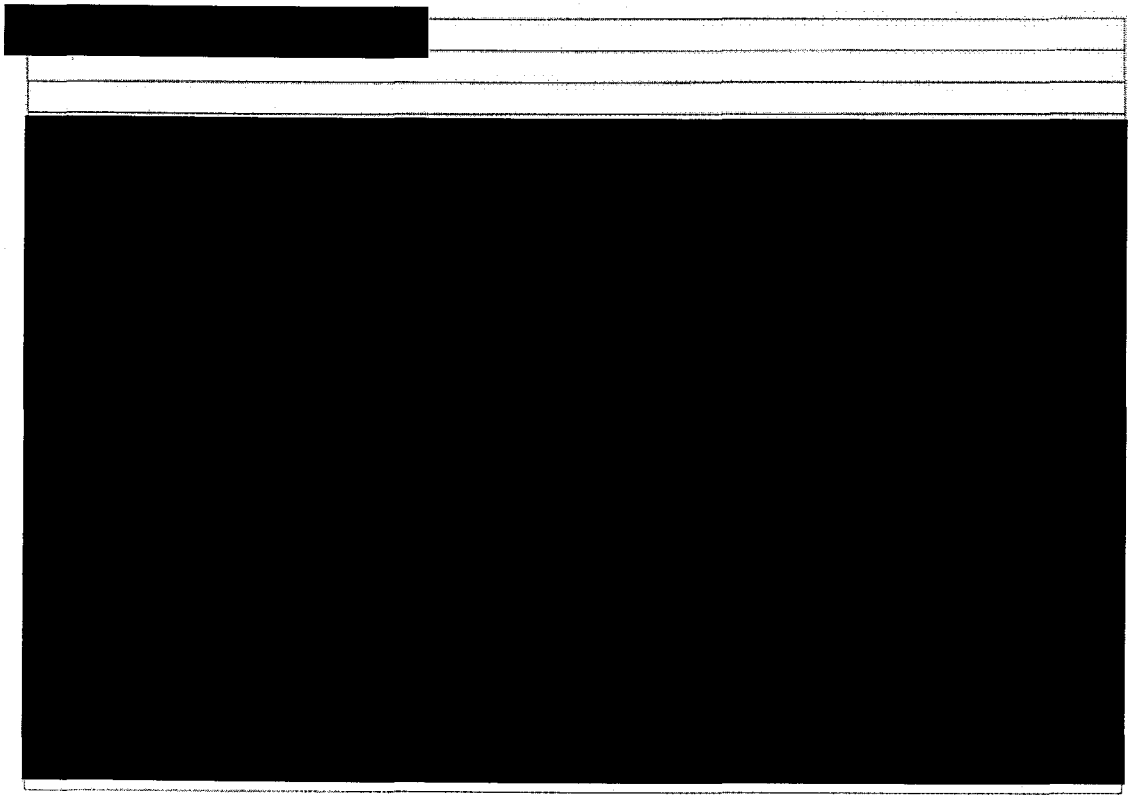


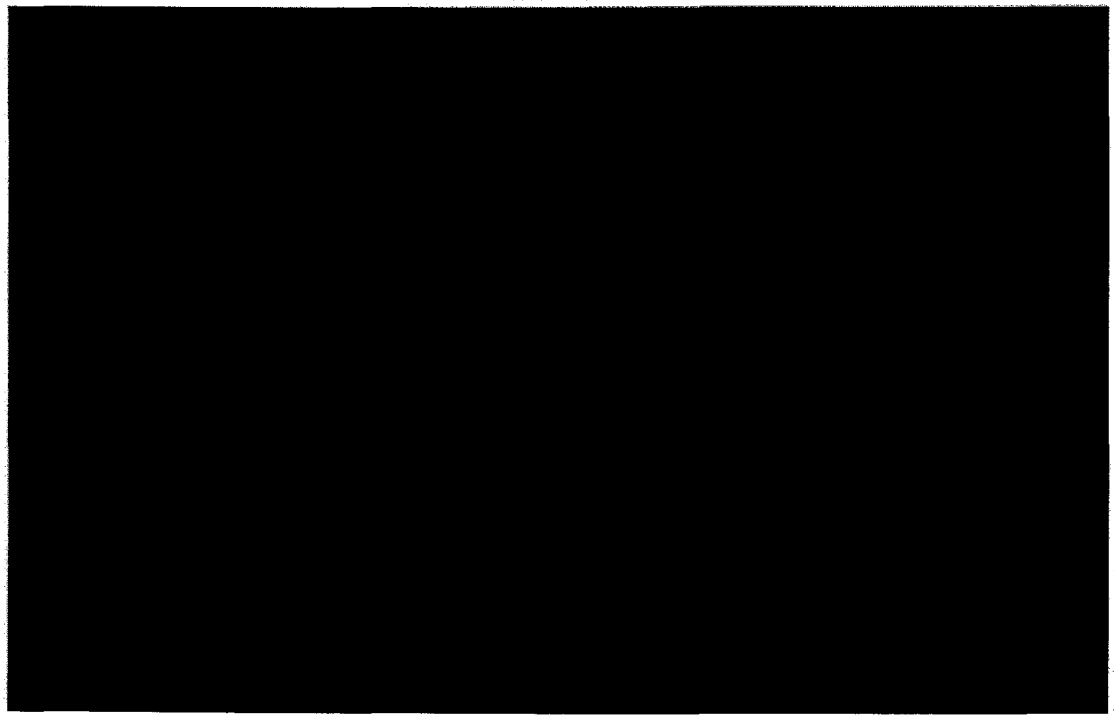












TAB

7

IAB [redacted]
2009 12 31 to 2015 07 31

[redacted]

Report #	Date Sent	[redacted]	Dissemination	Synopsis
[redacted]	2010 03 08	[redacted]		
	2010 04 26			
	2010 04 26			
	2010 08 04			
	2010 09 07			
	2010 09 08			

[redacted]			[redacted]
		2010 09 10	
		2010 09 10	
		2010 09 13	
		2010 09 13	
		2010 09 22	

[redacted]		2010 09 28	[redacted]
		2010 10 20	
		2010 12 16	
		2011 01 07	
		2011 01 12	
		2011 01 12	
		2011 01 12	

[redacted]		[redacted]
	2011 01 13	
	2011 01 28	
	2011 02 07	
	2011 02 25	
	2011 02 25	
	2011 03 01	
	2011 03 01	

[redacted]		2011 03 15	[redacted]
		2011 03 18	
		2011 03 28	
		2011 04 06	
		2011 04 08	
		2011 04 12	
		2011 04 13	

[redacted]	2011 04 21	[redacted]
	2011 04 26	
	2011 06 08	
	2011 06 13	
	2011 06 15	

			[redacted]
[redacted]		2011 06 17	
		2011 06 22	
		2011 06 22	
		2011 06 28	
		2011 06 30	

[redacted]		2011 06 30	[redacted]
		2011 06 30	
		2011 07 05	
		2011 07 07	

[redacted]		2011 07 08	[redacted]
		2011 07 13	
		2011 07 14	
		2011 07 14	

[redacted]	2011 07 15	[redacted]
	2011 08 08	
	2011 08 10	
	2011 08 22	

		[redacted]
[redacted]		2011 09 14
		2011 10 14
		2011 10 19
		2011 10 21

[redacted]		2011 11 08	[redacted]
		2011 11 08	
		2011 11 15	
		2011 11 15	
		2011 11 22	
		2011 12 22	
		2011 12 28	
		2011 12 29	
		2012 01 03	

		[redacted]
[redacted]	2012 01 04	
	2012 01 05	
	2012 01 09	

[redacted]		2012 01 09	[redacted]
		2012 01 10	
		2012 01 11	
		2012 01 11	

[redacted]		2012 01 11	[redacted]
		2012 01 19	
		2012 01 20	
		2012 01 25	
		2012 02 22	

[redacted]	2012 03 21	[redacted]
	2012 05 28	
	2012 06 01	
	2012 07 05	
	2012 07 10	
	2012 07 16	

[redacted]		2012 08 27	[redacted]
		2013 04 24	
		2013 04 25	
		2013 04 25	
		2013 05 22	
		2013 07 18	
		2013 08 07	

		[redacted]
[redacted]	2013 08 09	
	2013 08 21	
	2013 10 25	
	2013 10 31	

[redacted]	2014 01 07	[redacted]
	2014 05 01	
	2014 06 03	
	2014 06 05	
	2014 06 19	
	2014 07 22	
	2014 12 11	
	2014 12 19	

[redacted]		2015 06 18	[redacted]
		2015 07 10	

	A	B	C	D	E
1	Report #	Date Sent	[redacted]	Dissemination	Synopsis
2	[redacted]	2010 03 08	[redacted]	[redacted]	[redacted]
3	[redacted]	2010 04 26	[redacted]	[redacted]	[redacted]
4	[redacted]	2010 04 26	[redacted]	[redacted]	[redacted]
5	[redacted]	2010 08 04	[redacted]	[redacted]	[redacted]
6	[redacted]	2010 09 07	[redacted]	[redacted]	[redacted]
7	[redacted]	2010 09 08	[redacted]	[redacted]	[redacted]
8	[redacted]	2010 09 10	[redacted]	[redacted]	[redacted]
9	[redacted]	2010 09 10	[redacted]	[redacted]	[redacted]
10	[redacted]	2010 09 13	[redacted]	[redacted]	[redacted]
11	[redacted]	2010 09 13	[redacted]	[redacted]	[redacted]
12	[redacted]	2010 09 22	[redacted]	[redacted]	[redacted]
13	[redacted]	2010 09 28	[redacted]	[redacted]	[redacted]
14	[redacted]	2010 30 20	[redacted]	[redacted]	[redacted]
15	[redacted]	2010 12 16	[redacted]	[redacted]	[redacted]
16	[redacted]	2011 01 07	[redacted]	[redacted]	[redacted]
17	[redacted]	2011 01 12	[redacted]	[redacted]	[redacted]
18	[redacted]	2011 01 12	[redacted]	[redacted]	[redacted]
19	[redacted]	2011 01 12	[redacted]	[redacted]	[redacted]
20	[redacted]	2011 01 13	[redacted]	[redacted]	[redacted]
21	[redacted]	2011 01 28	[redacted]	[redacted]	[redacted]
22	[redacted]	2011 02 07	[redacted]	[redacted]	[redacted]

	A	B	C	D	E
23	[redacted]	2011 02 25	[redacted]		
24		2011 02 25			
25		2011 03 01			
26		2011 03 01			
27		2011 03 15			
28		2011 03 18			
29		2011 03 28			
30		2011 04 06			
31		2011 04 08			
32		2011 04 12			
33		2011 04 13			
34		2011 04 21			
35		2011 04 26			
36		2011 06 08			
37		2011 06 13			
38		2011 06 15			
39		2011 06 17			
40		2011 06 22			
41		2011 06 22			
42		2011 06 28			
43		2011 06 30			

[redacted] Tab/Onglet 3 Page 55

	A	B	C	D	E
44	[redacted]	2011 06 30	[redacted]		
45		2011 06 30			
46		2011 07 05			
47		2011 07 07			
48		2011 07 06			
49		2011 07 13			
50		2011 07 14			
51		2011 07 14			
52		2011 07 15			
53		2011 08 08			
54		2011 08 10			
55		2011 08 22			
56		2011 09 14			
57		2011 10 14			
58		2011 10 19			
59		2011 10 21			

	A	B	C	D	E
60	[redacted]	2011 11 08	[redacted]		
61		2011 11 08			
62		2011 11 15			
63		2011 11 15			
64		2011 11 22			
65		2011 12 22			
66		2011 12 28			
67		2011 12 29			
68		2012 01 03			
69		2012 01 04			
70		2012 01 05			
71		2012 01 09			
72		2012 01 09			
73		2012 01 10			
74		2012 01 11			
75		2012 01 11			
76		2012 01 11			

	A	B	C	D	E
77	[redacted]	2012 01 19	[redacted]		
78		2012 01 20			
79		2012 01 25			
80		2012 02 22			
81		2012 03 21			
82		2012 05 28			
83		2012 06 01			
84		2012 07 05			
85		2012 07 10			
86		2012 07 16			
87		2012 08 27			
88		2013 04 24			
89		2013 04 25			
90		2013 04 25			
91		2013 05 22			
92		2013 07 18			
93		2013 08 07			
94		2013 08 09			
95		2013 08 21			
96		2013 10 25			

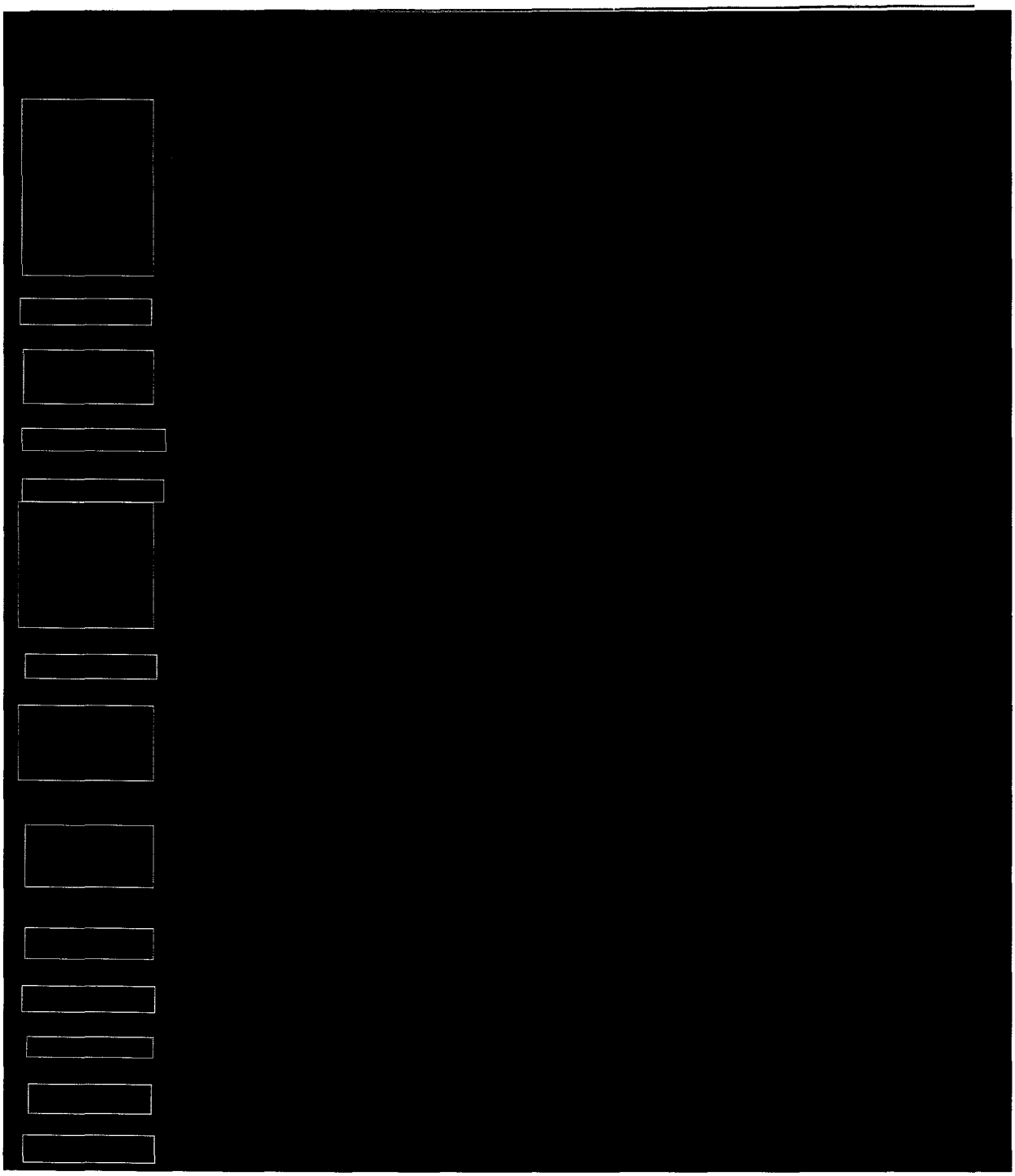
	A	B	C	D	E
97	[redacted]	2013 10 31	[redacted]	[redacted]	[redacted]
98		2014 01 07			
99		2014 05 01			
100		2014 06 03			
101		2014 06 05			
102		2014 06 19			
103		2014 07 22			
104		2014 12 11			
105		2014 12 19			
106		2015 06 18			
107		2015 07 10			
108					
109					

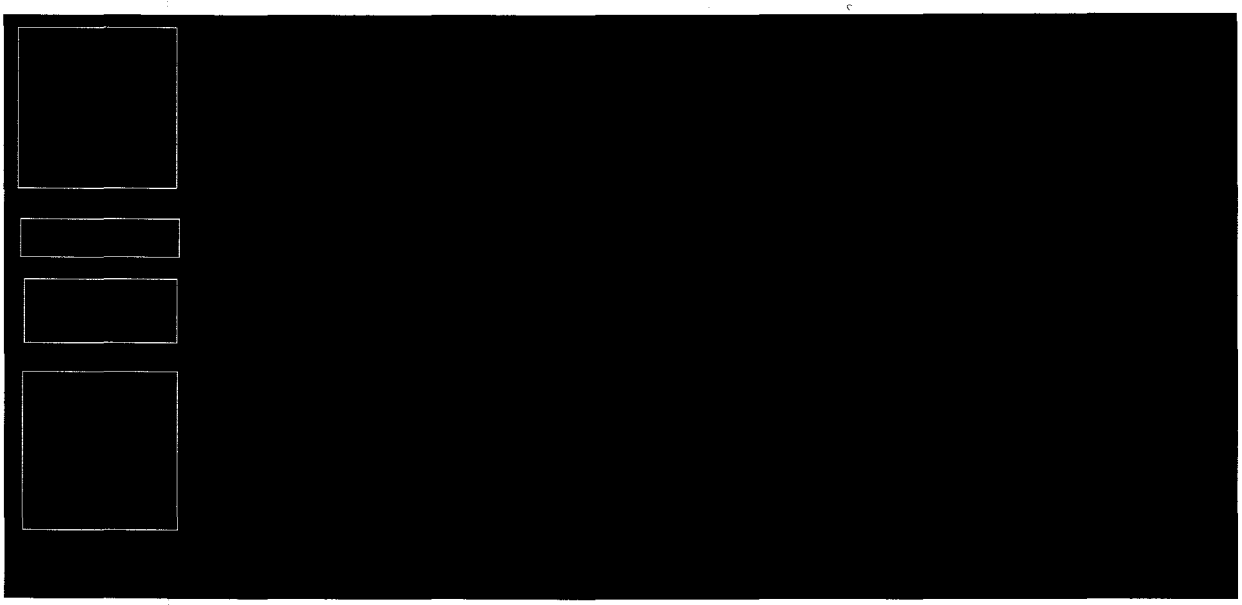
[redacted] Tab/Cahier 3 Page 59

TAB

4

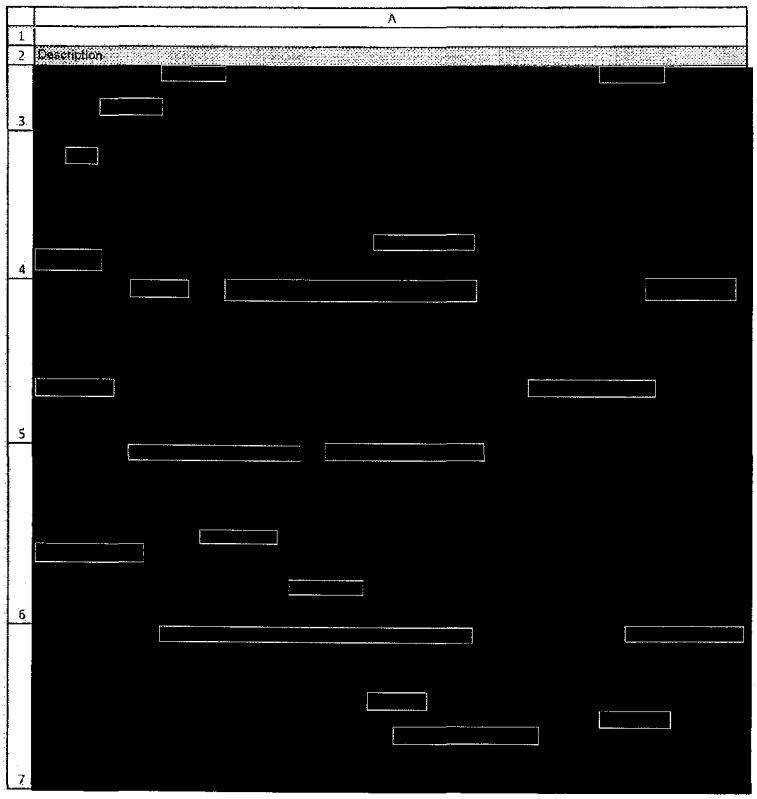
From: Unspecified Sender
Sent:
To:
Subject:



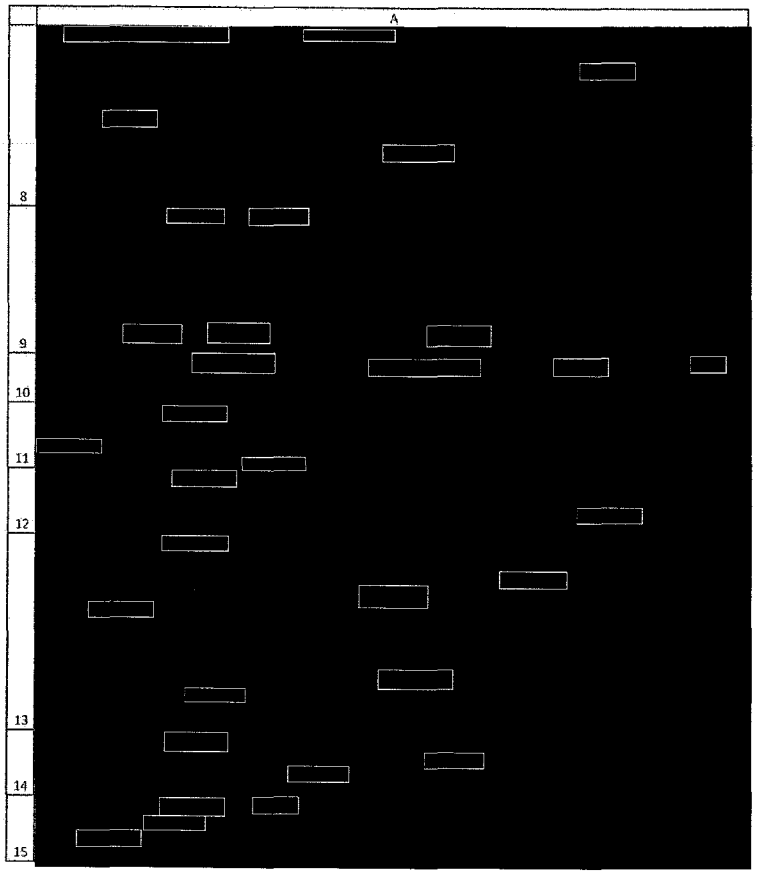


TAB

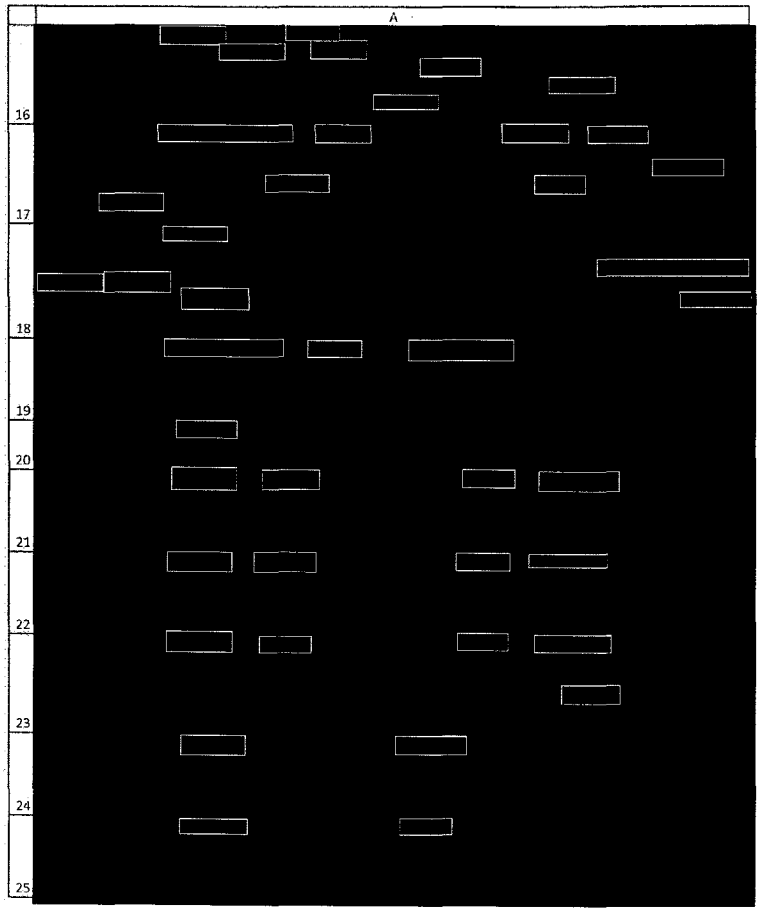
6



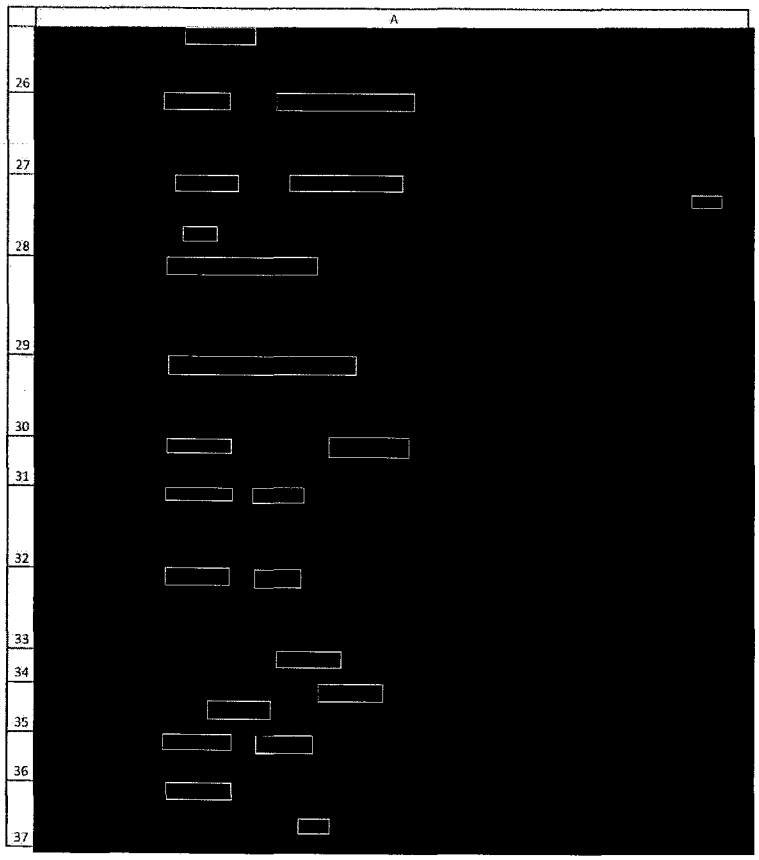
[redacted]



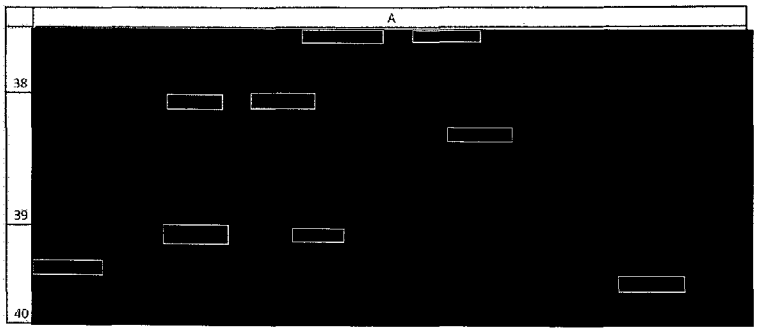
[redacted] Tab/Applet 6 Page 207



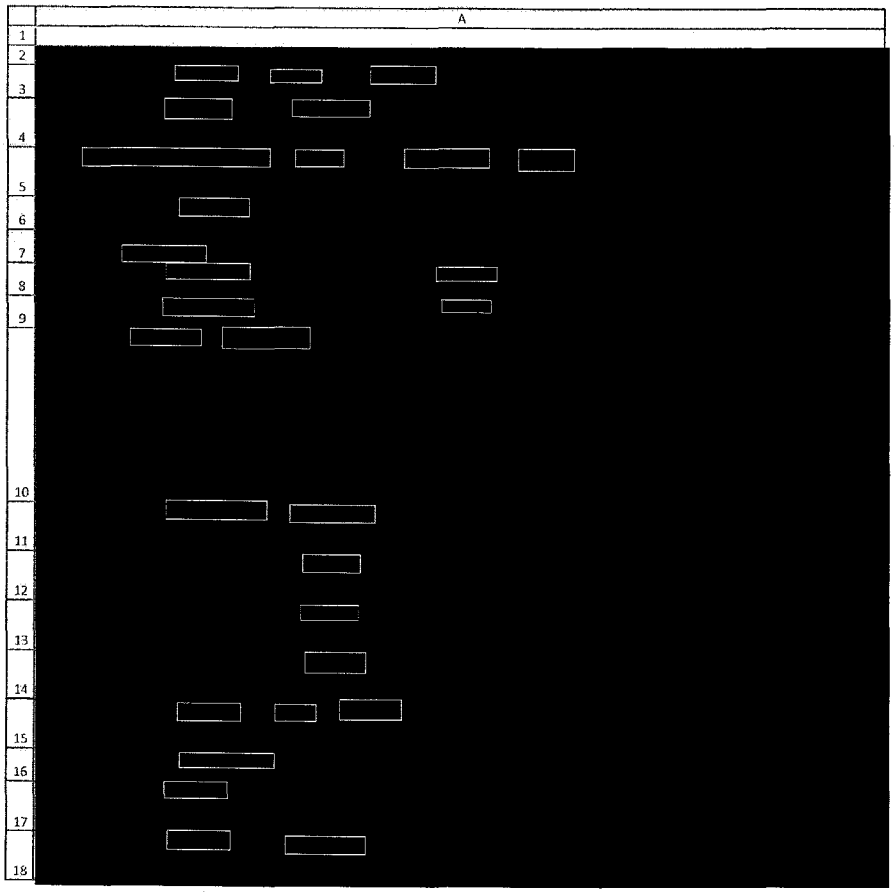
[redacted]



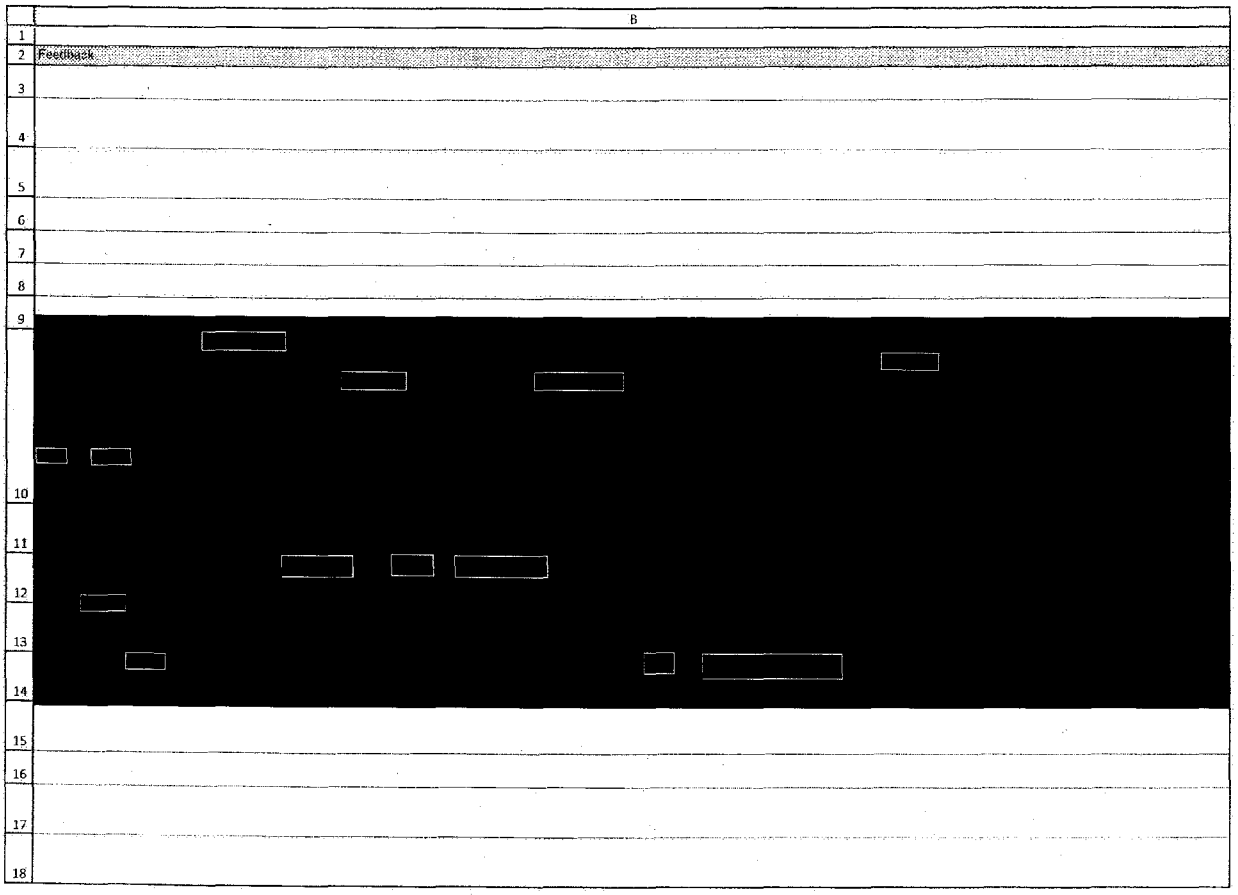
[redacted] Tab/Applet 6 Page 390



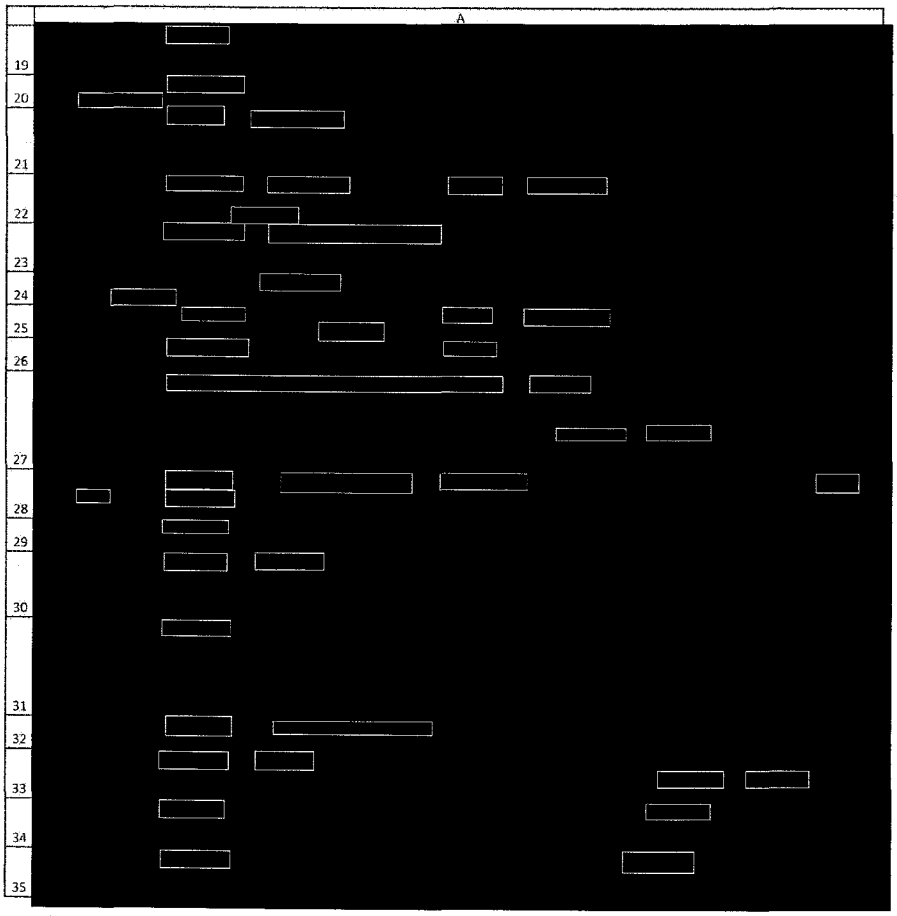
[redacted]



[redacted] Tab/Applet 6 Page 401



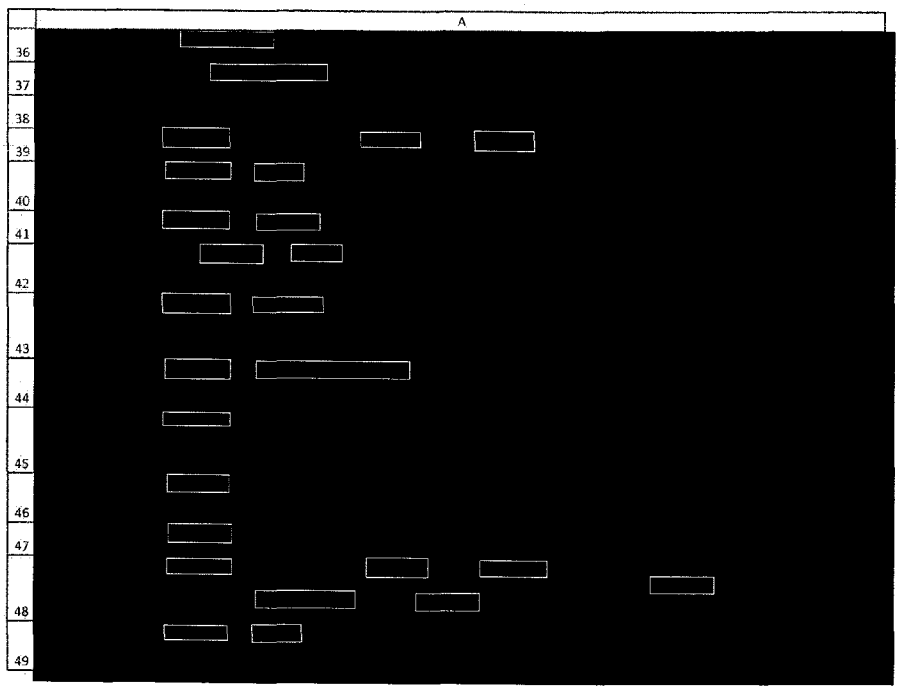
[redacted]



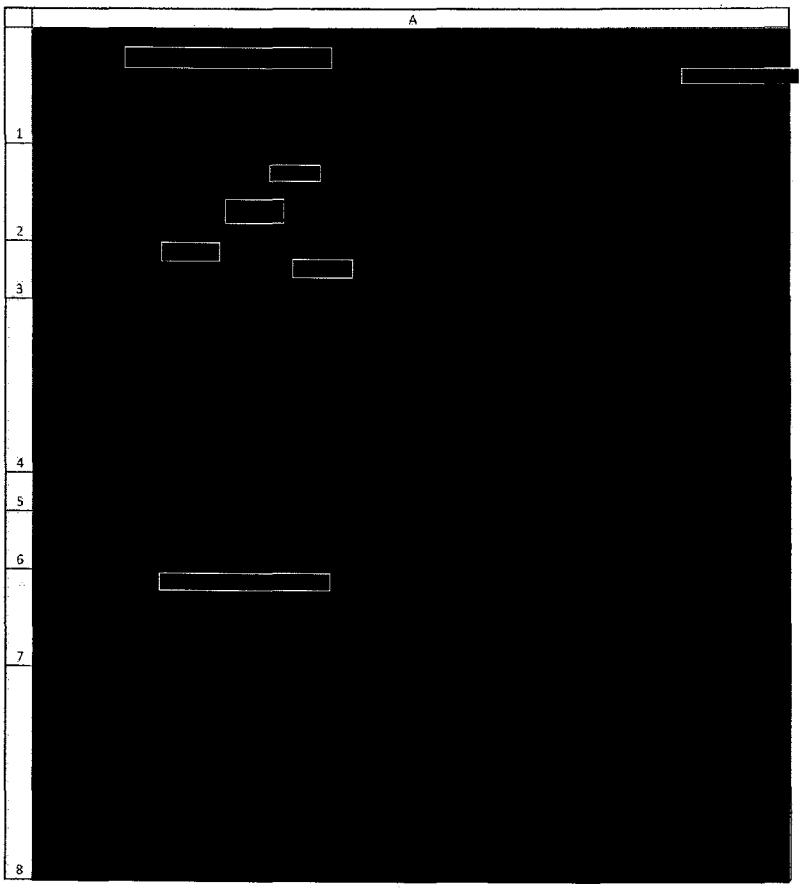
[redacted]

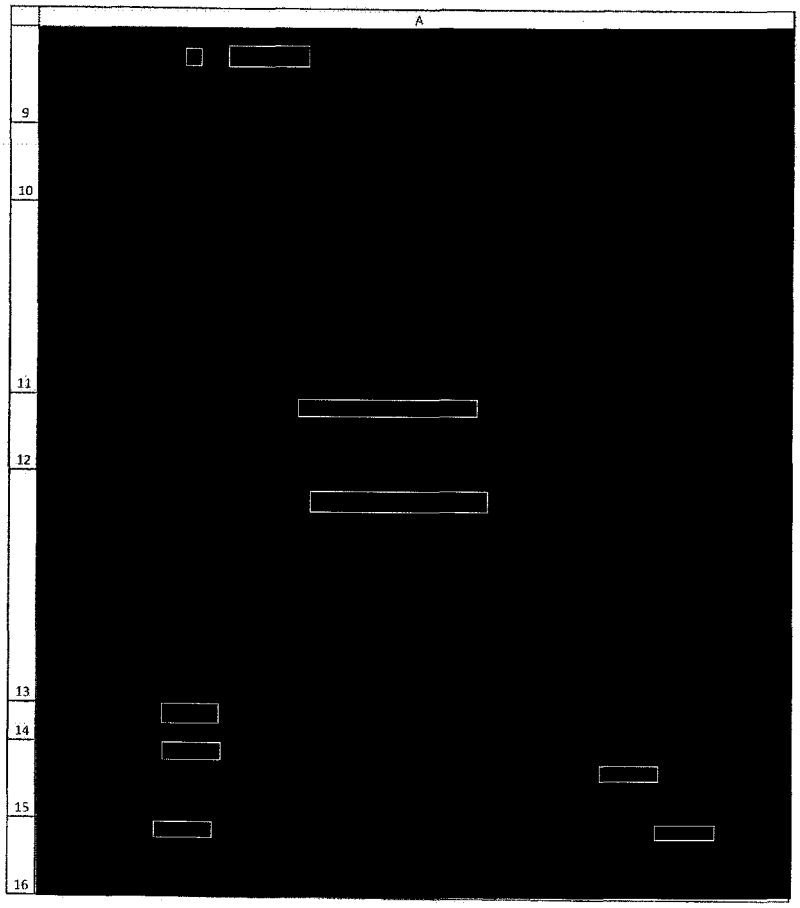
	B
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	

[redacted]

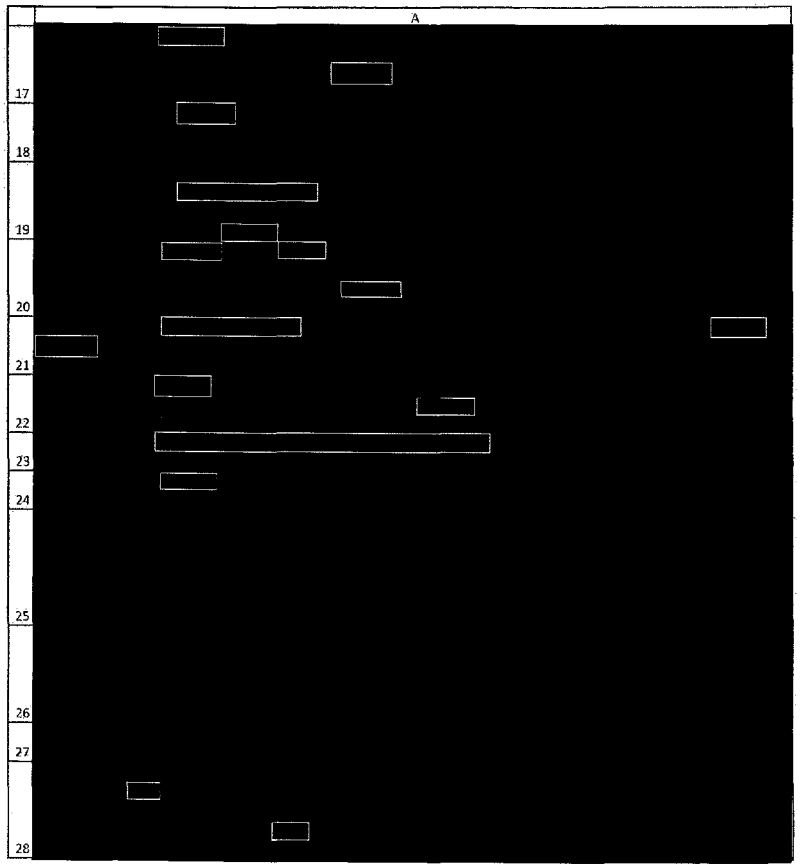


[redacted] Tab/Onglet 6 Page 405

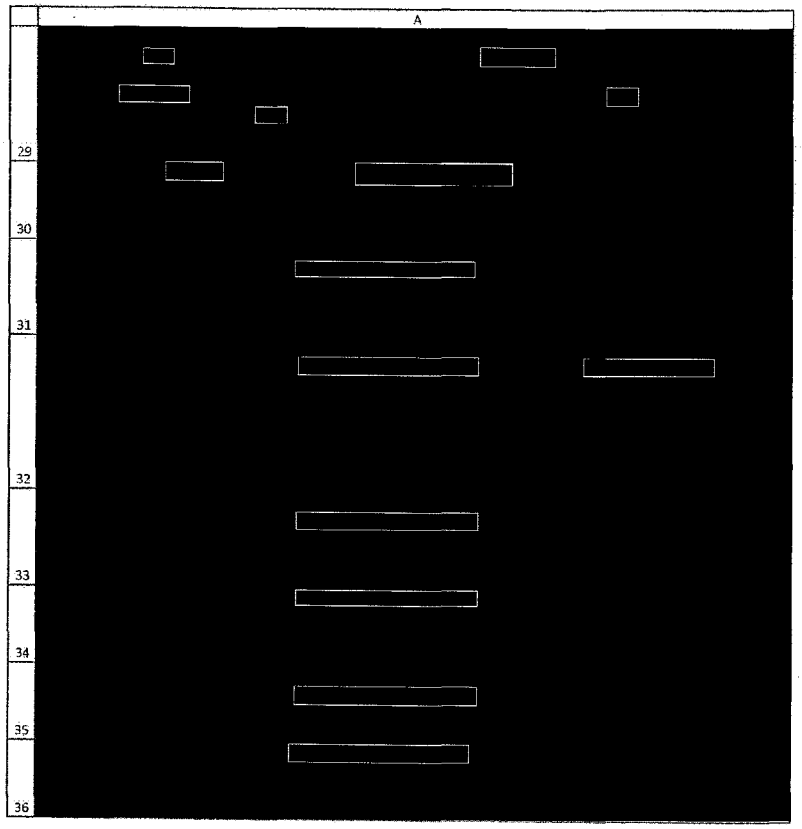

A
1
2
3
4
5
6
7
8



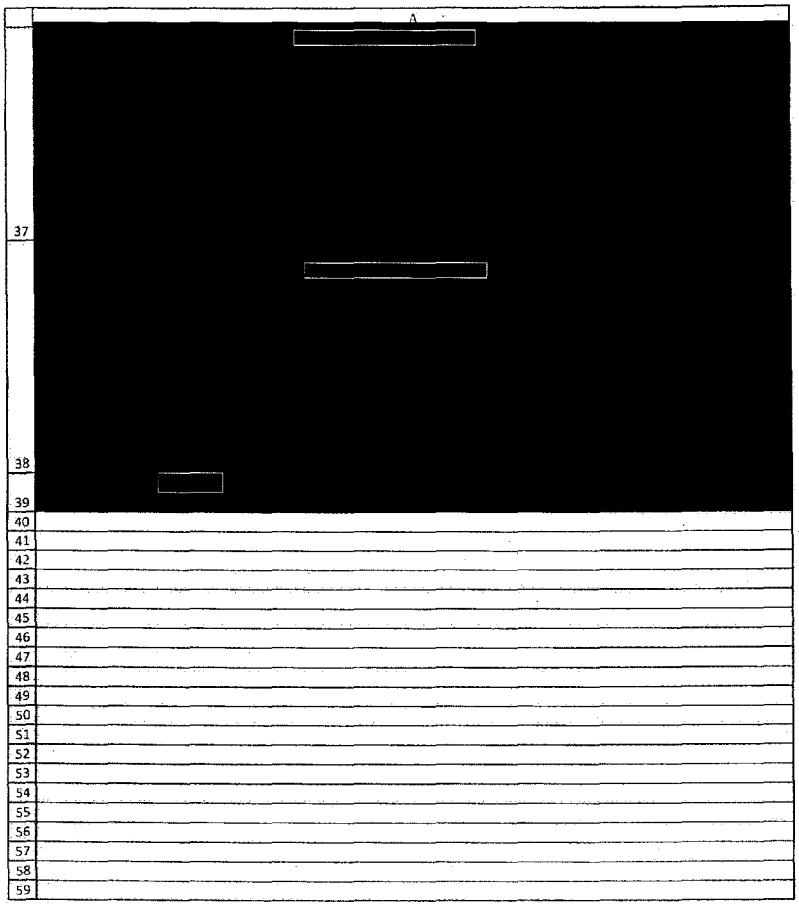
[redacted]



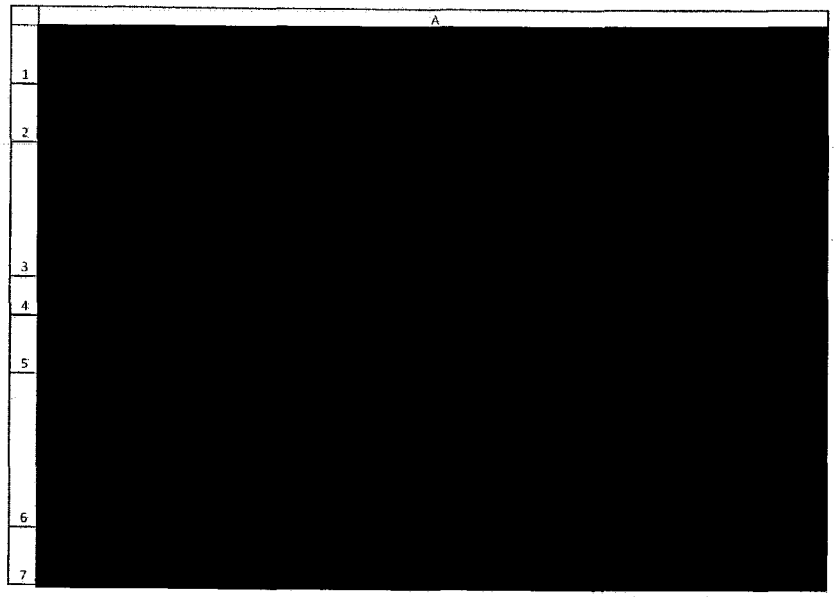
[redacted]



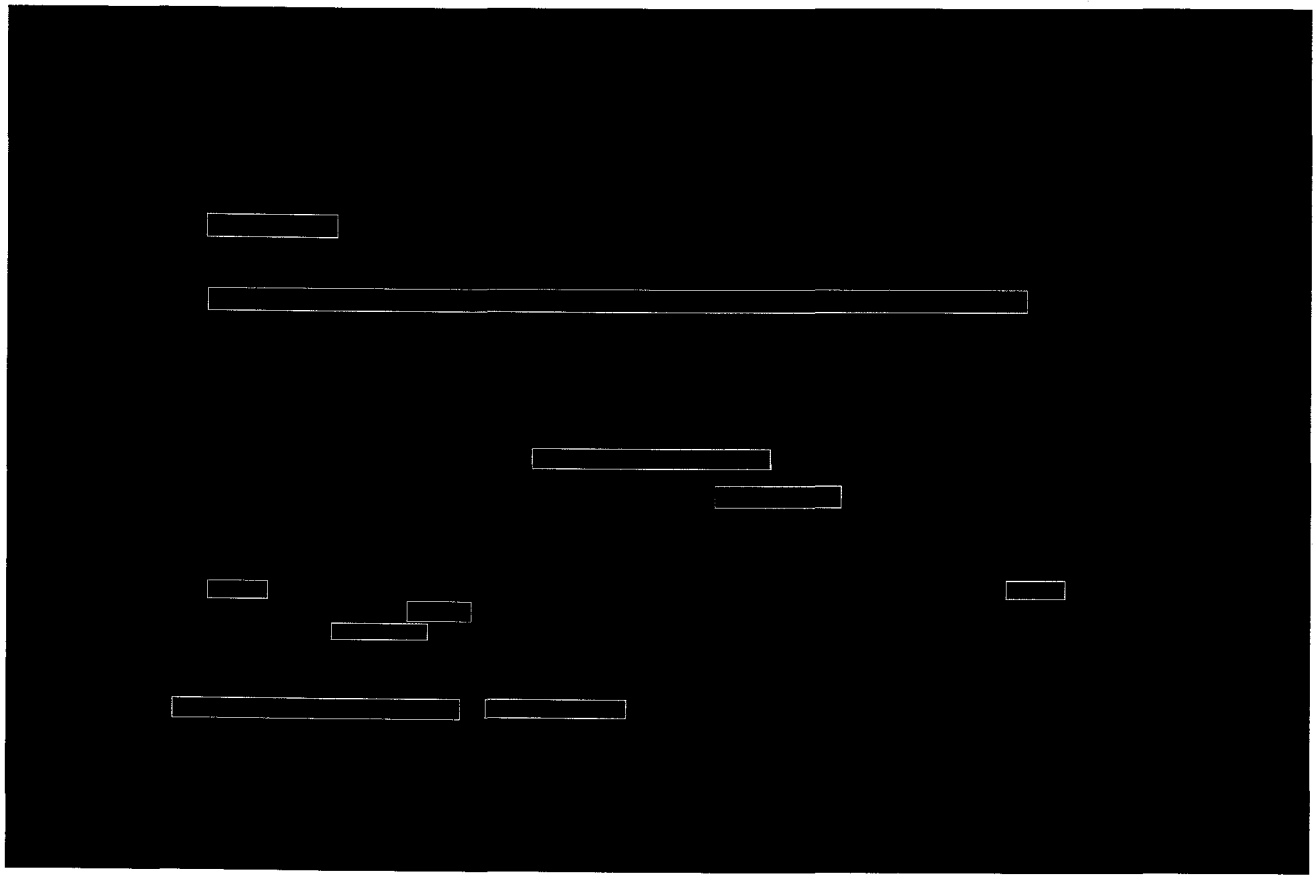
[redacted]

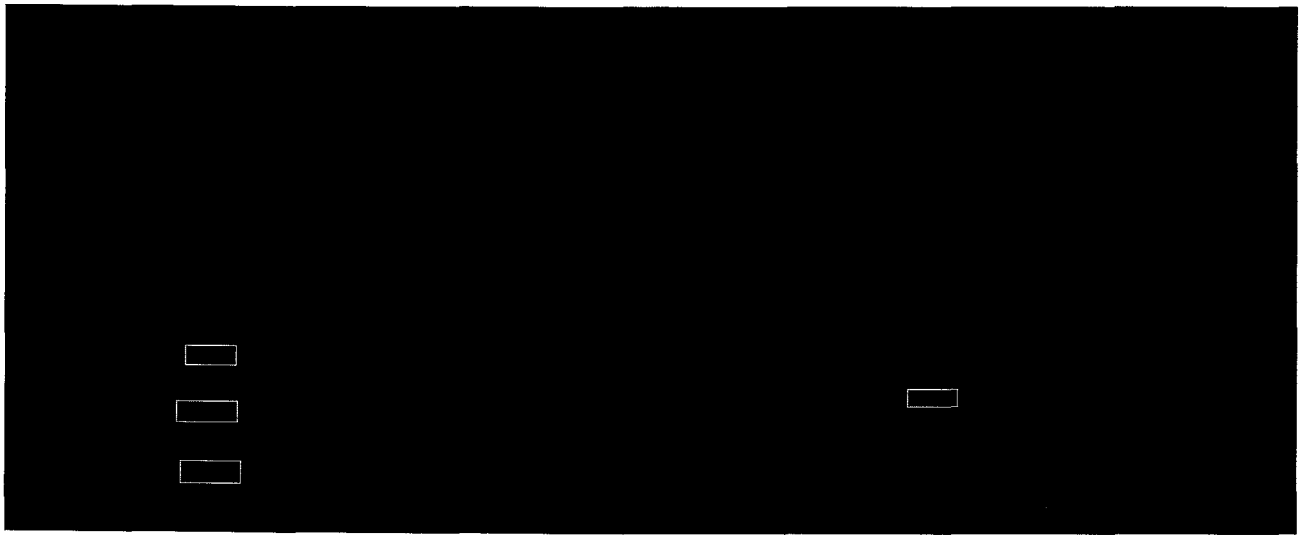


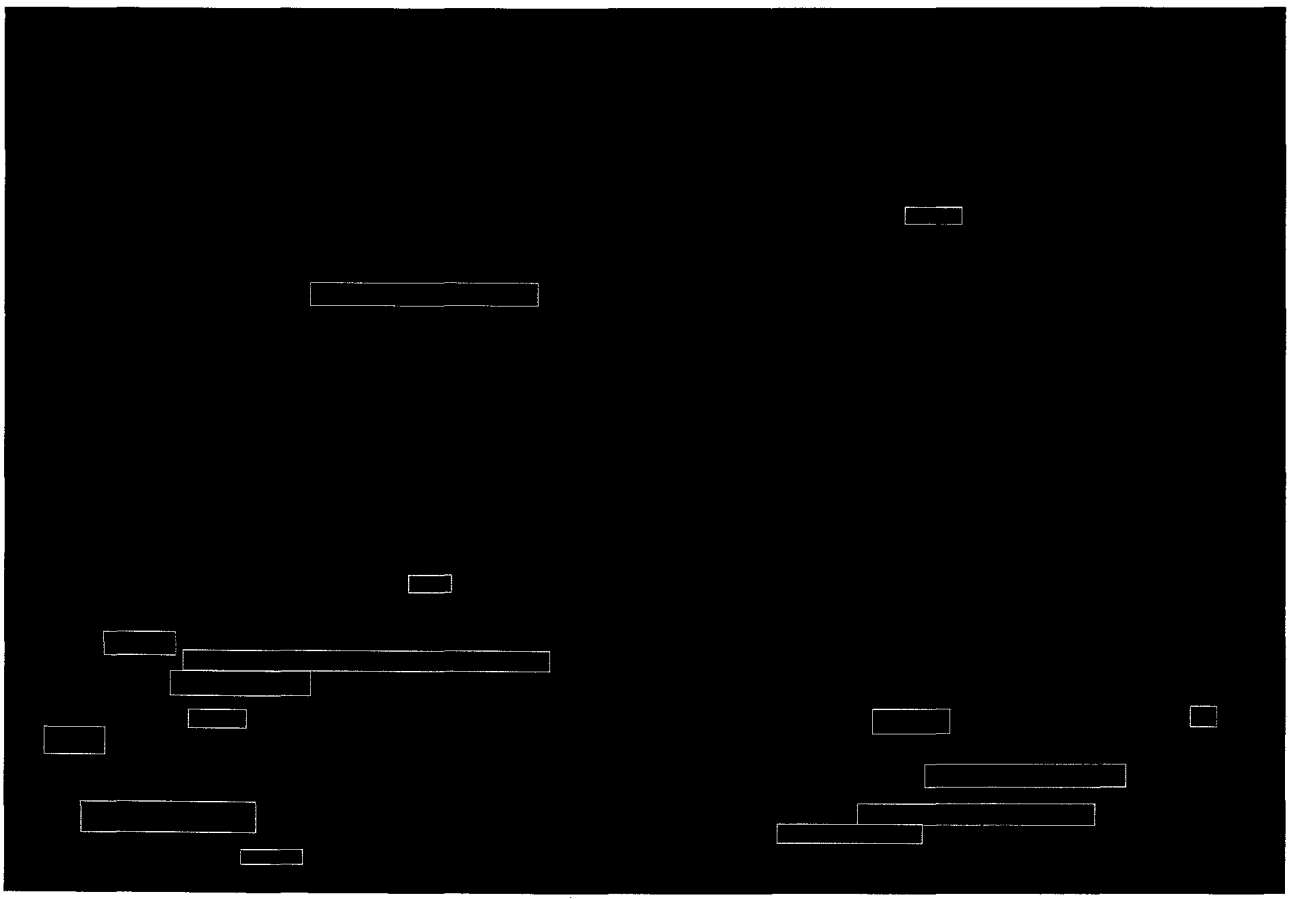
[redacted]

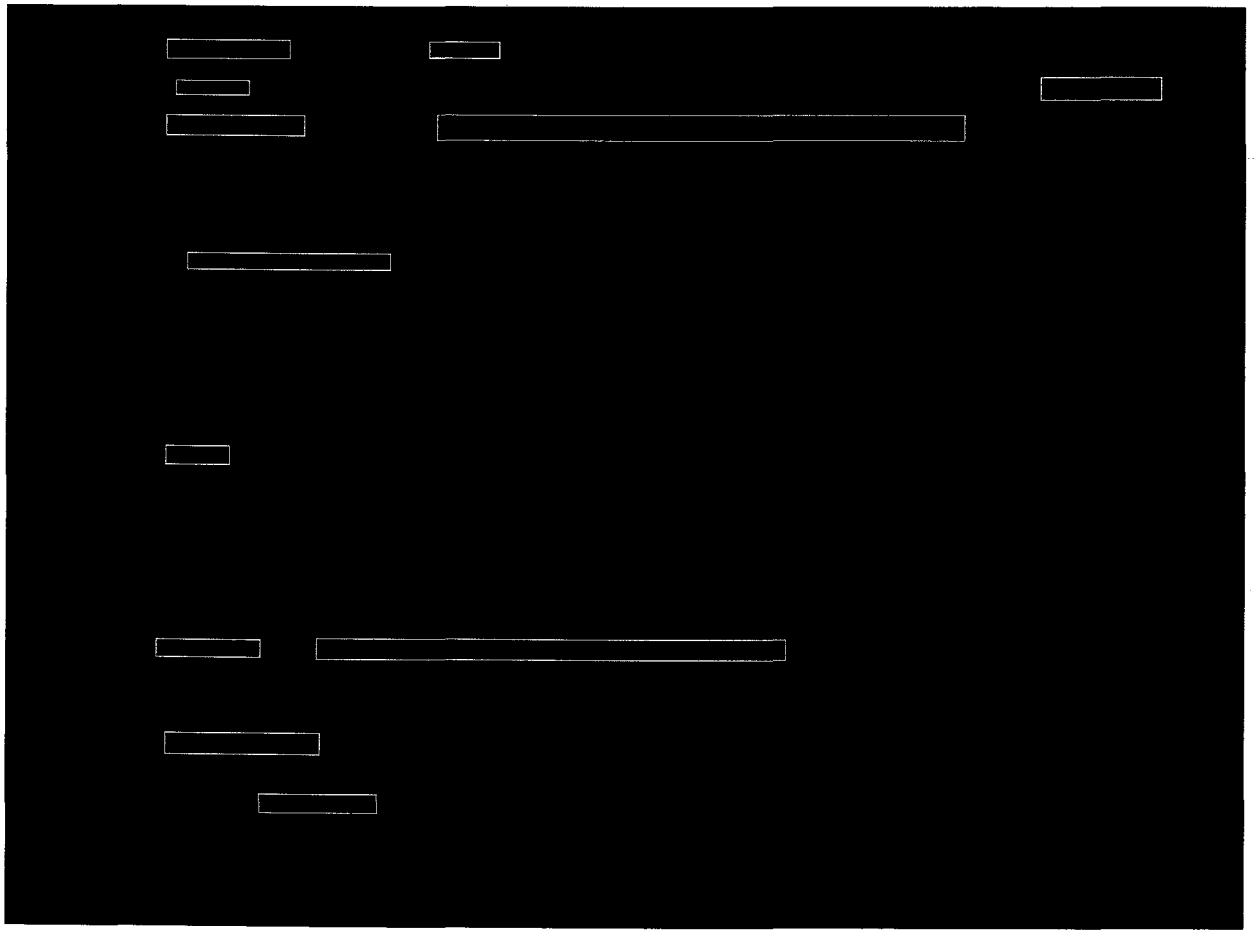


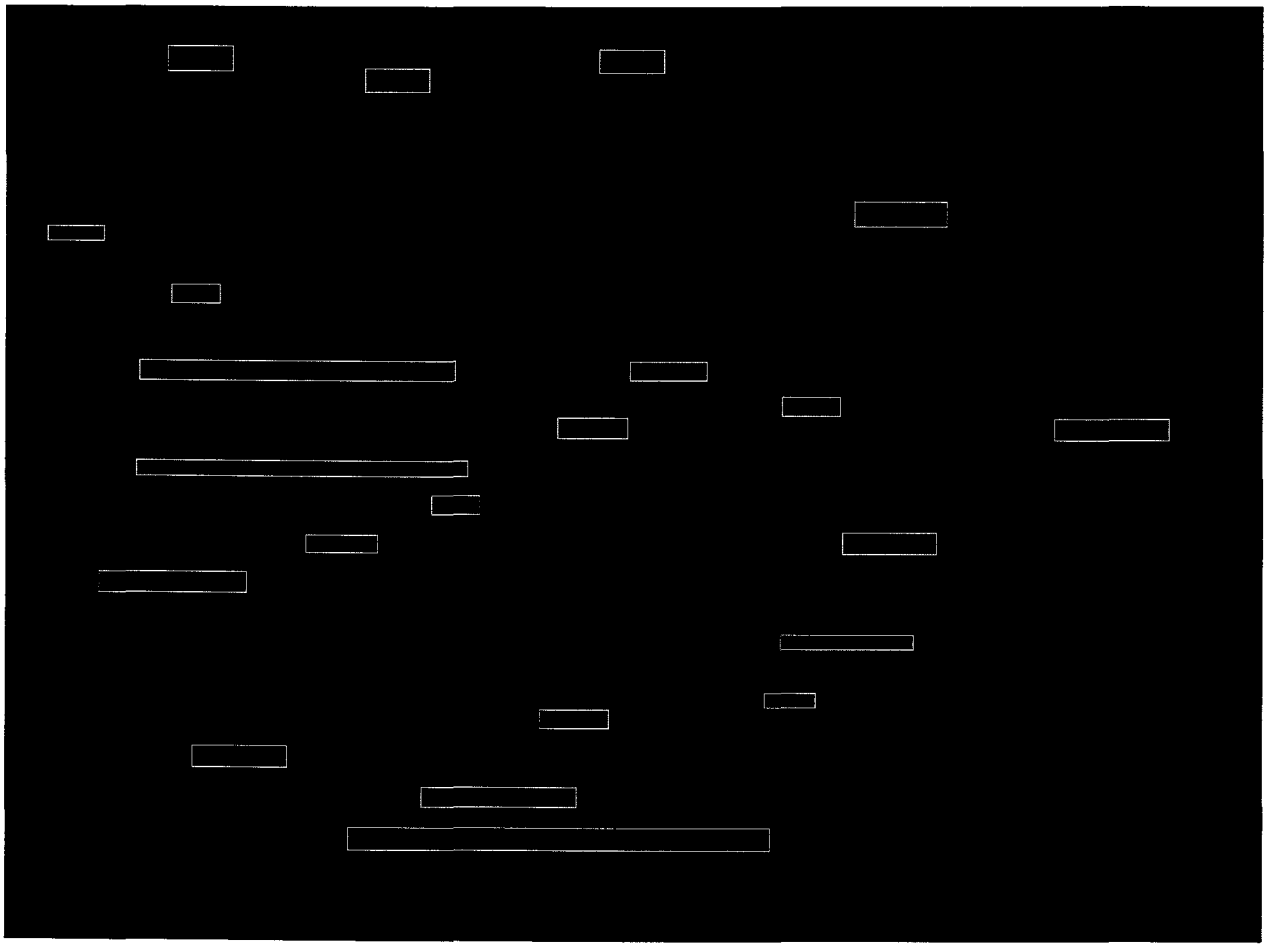
[redacted]

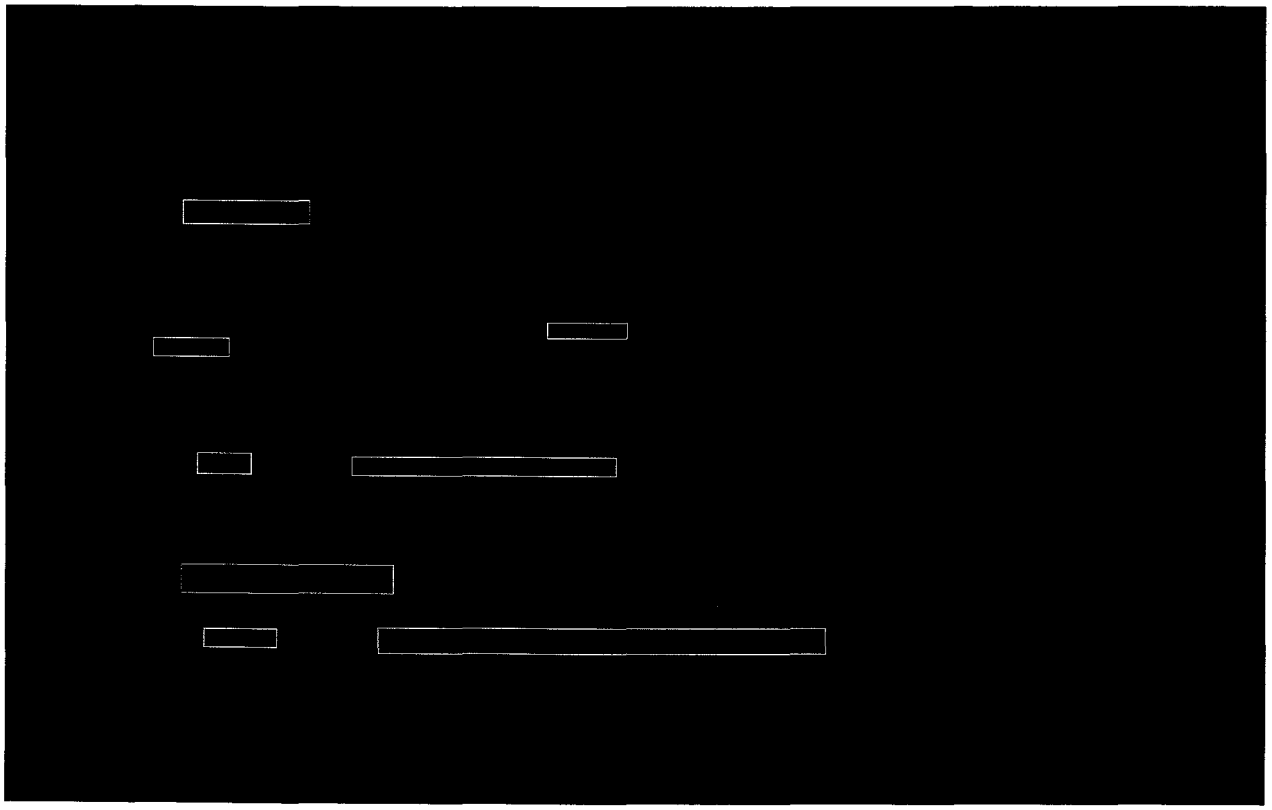


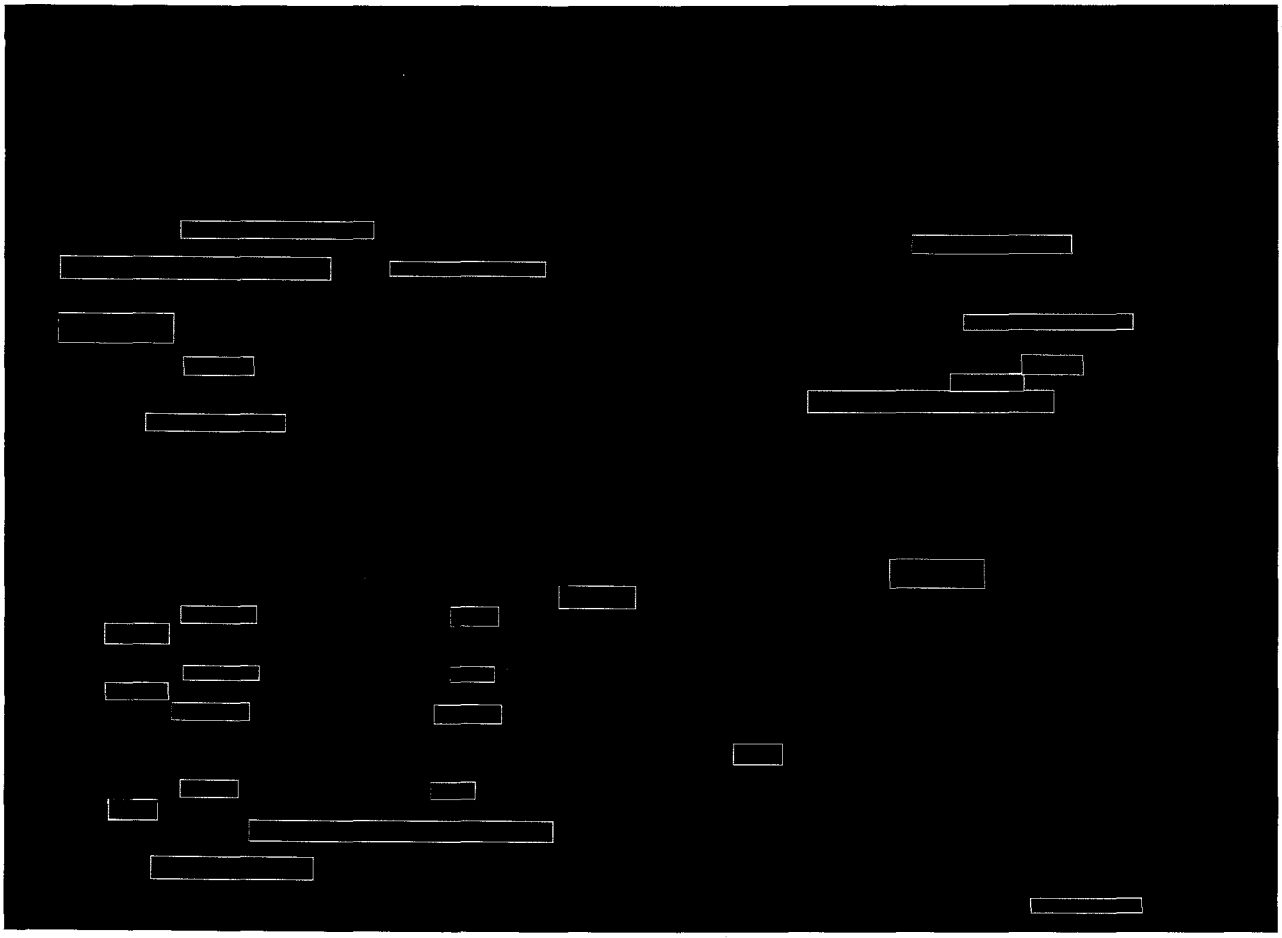


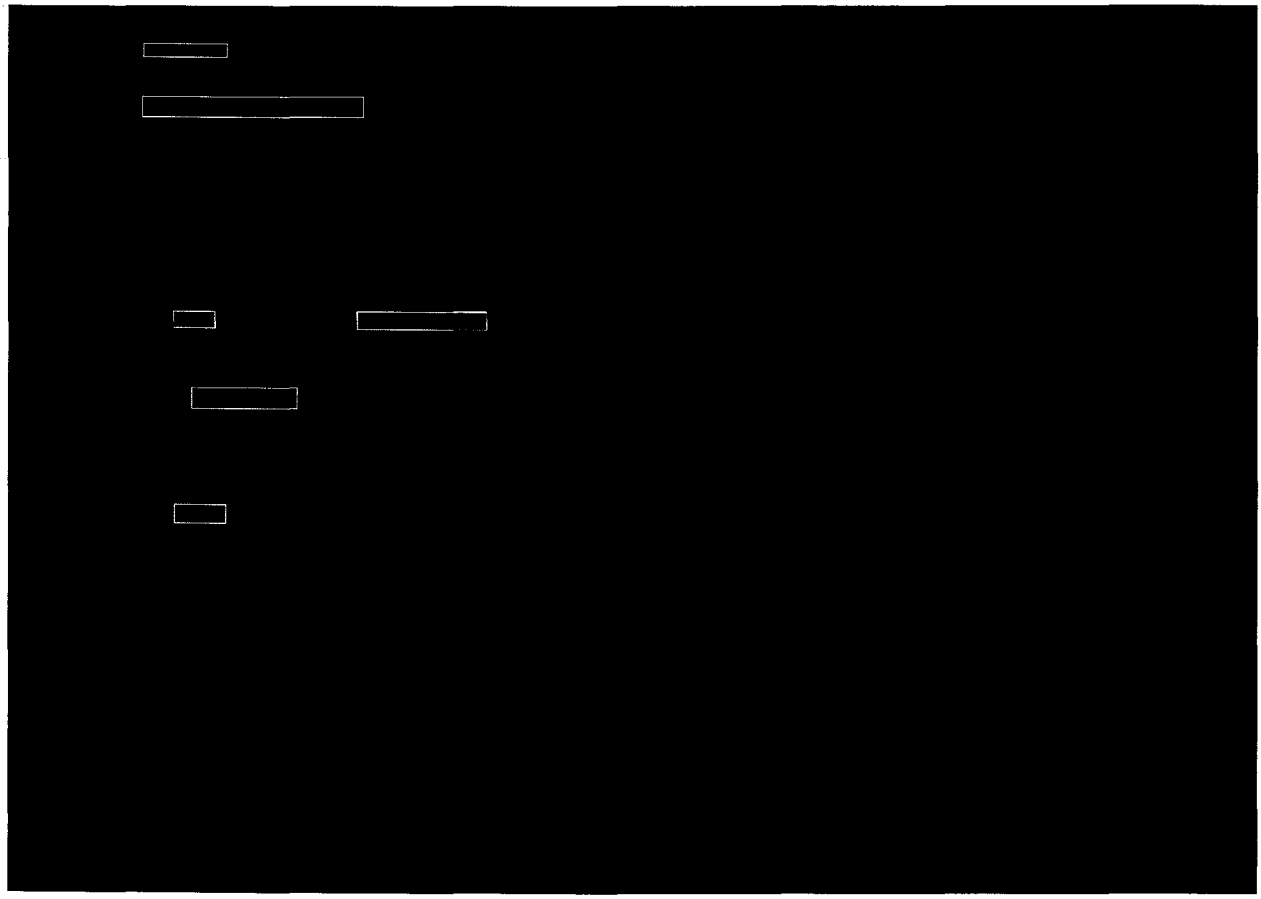


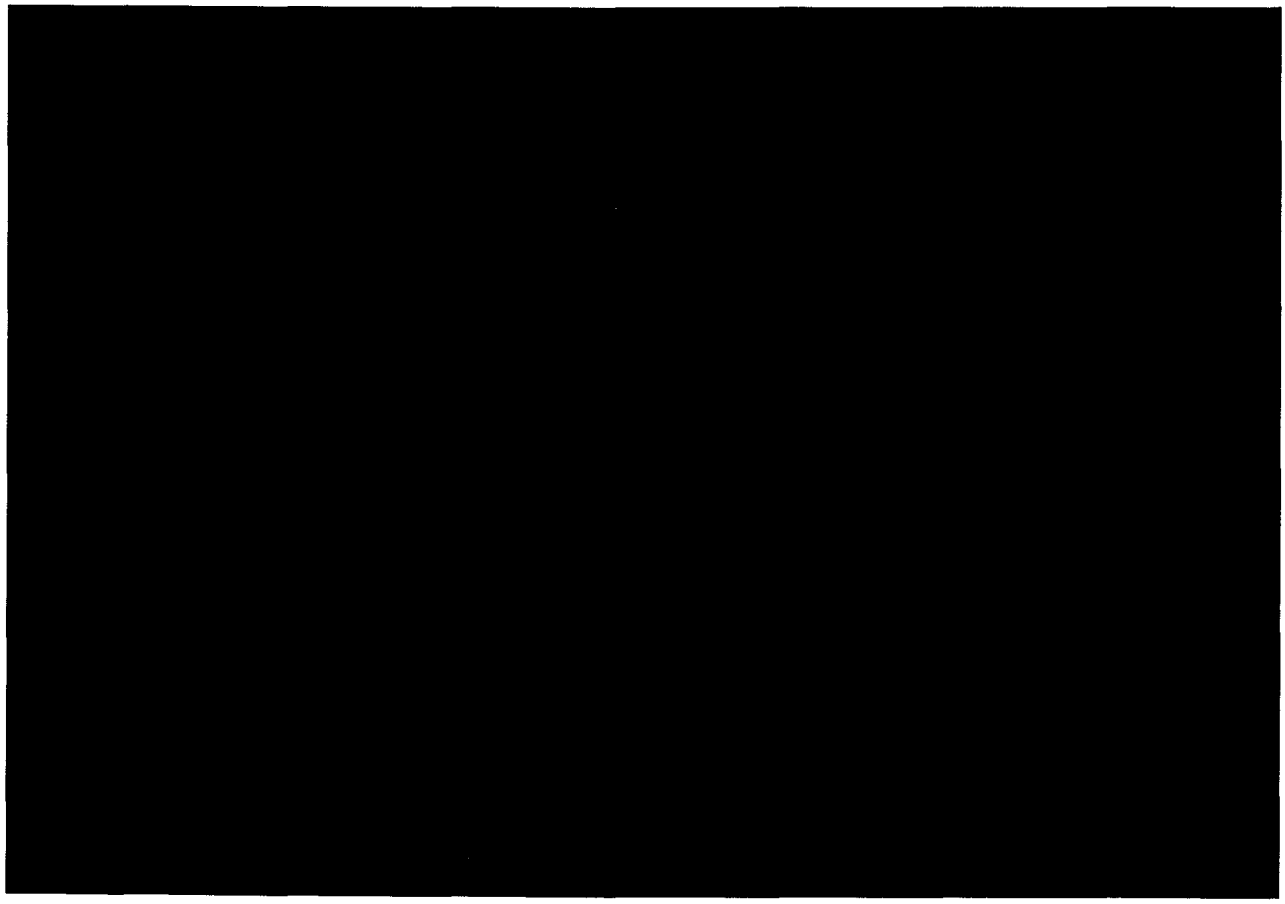












[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, November 24, 2015 10:40 AM
To: [redacted]
Subject: As discussed
Attach: IAB CONTACT REPORT 25.docx; IAB CONTACT REPORT 13.docx

Classification: Secret
Classification: Secret
Not for PA / Ne pas classer

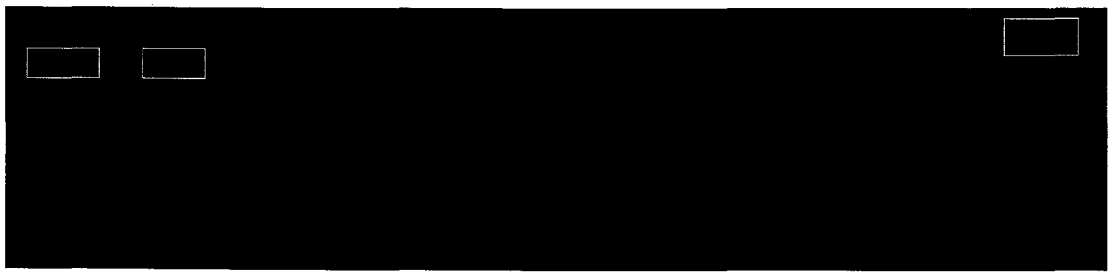
SUBJECT Briefing to Deputy Premier, Province of New Brunswick (PNB) – [redacted] - Briefings, Presentations and Advice to GoC

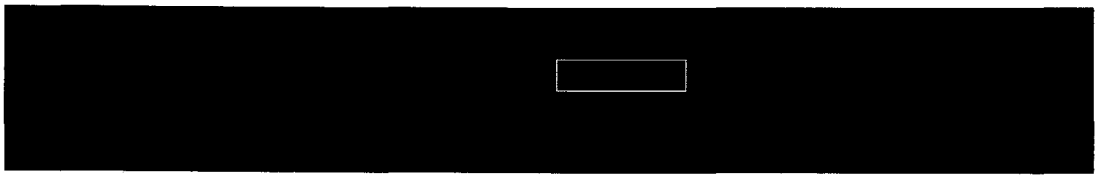
UNIT [redacted]

ISSUE On 2015-07-20 an IAB Strategic Analyst and the RDG-AR delivered a 30 minute presentation to the Deputy Premier, GNB (also Minister of Public Safety and Justice), the DM and DG of Public Safety, GNB. The Assistant Commissioner and Superintendent (J Division RCMP) also attended. [redacted] A group discussion and Q&A followed the presentation. The GNB representatives were very thankful for the briefing.

ACTION IAB continues to support our partners and our regional offices.

[redacted]





TAB

8

Canadian Security Intelligence Service

Intelligence Requirements
2009/2010

List of Intelligence Requirements 2009/10

INTELLIGENCE REQUIREMENTS 2009/10 - PROCEDURES

[redacted]

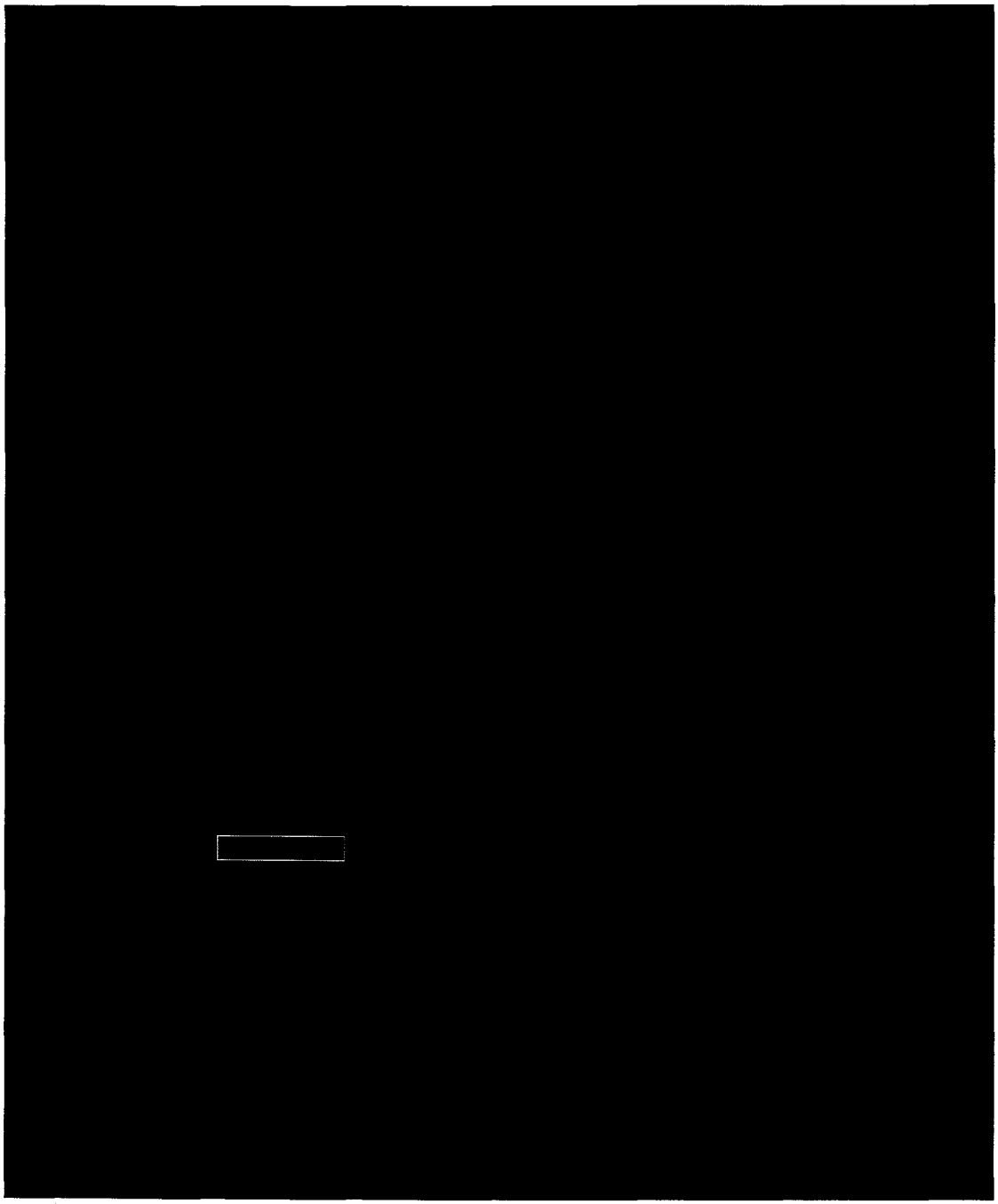
1

Other Considerations:

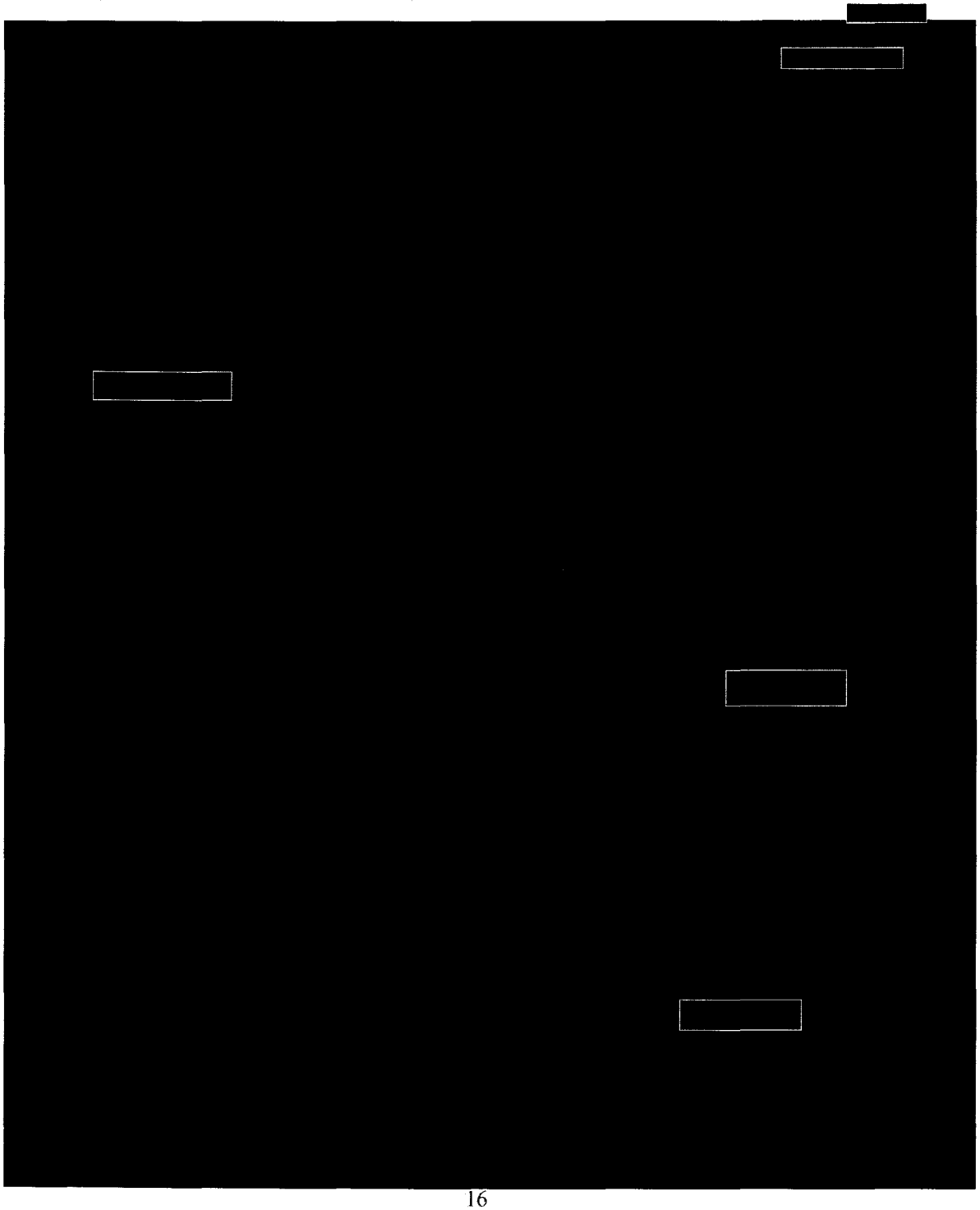
[redacted]

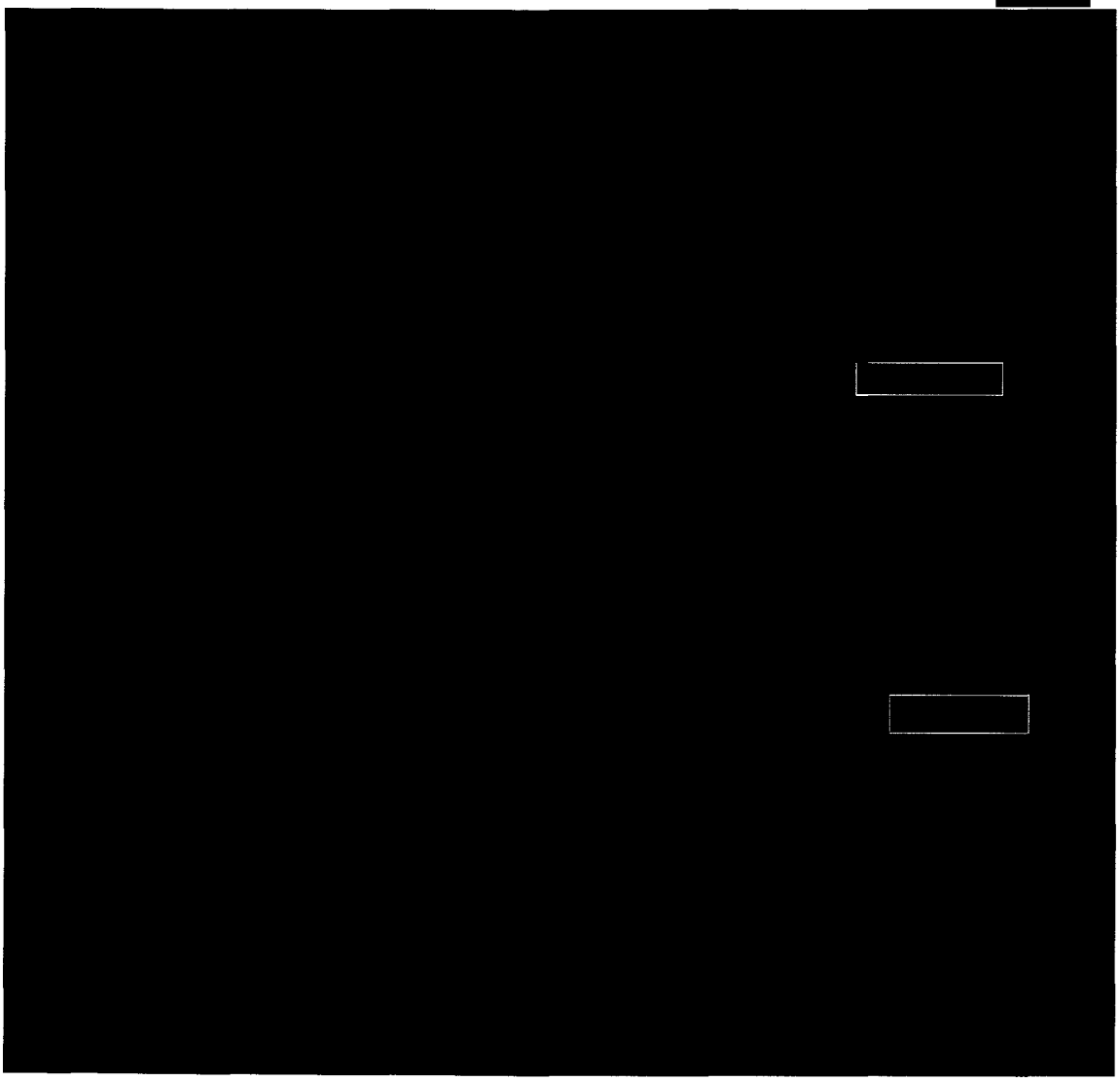
We would ask that questions or concerns from the Regions be coordinated through the respective DDG Ops. The IAB point of contact will be [redacted] DDG IAB[redacted]

[redacted]



15





Secret CEO

Canadian Security Intelligence Service

Intelligence Requirements
2010/2011

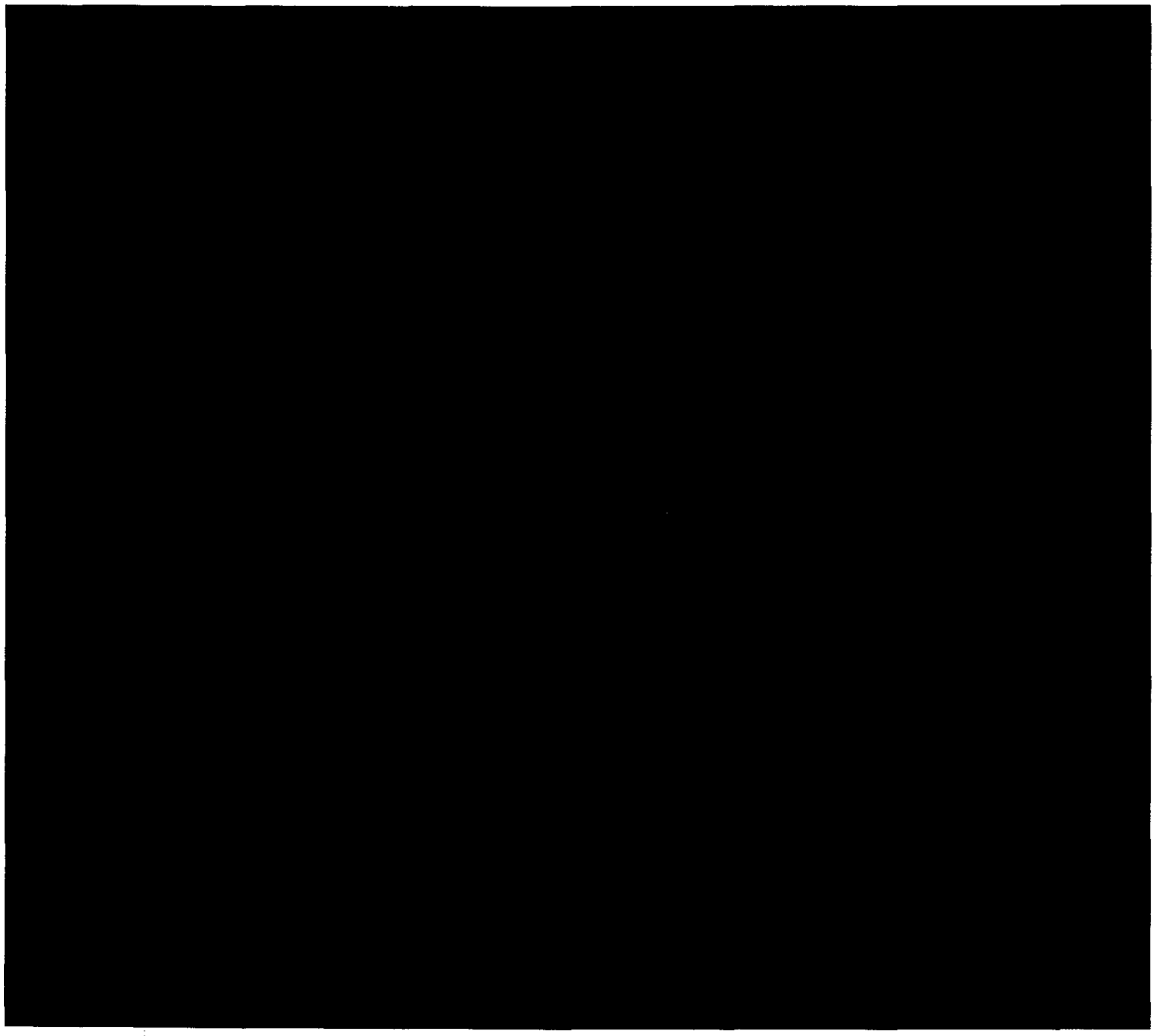
[redacted]

List of Intelligence Requirements 2009/10

INTELLIGENCE REQUIREMENTS 2010/2011 - PROCEDURES

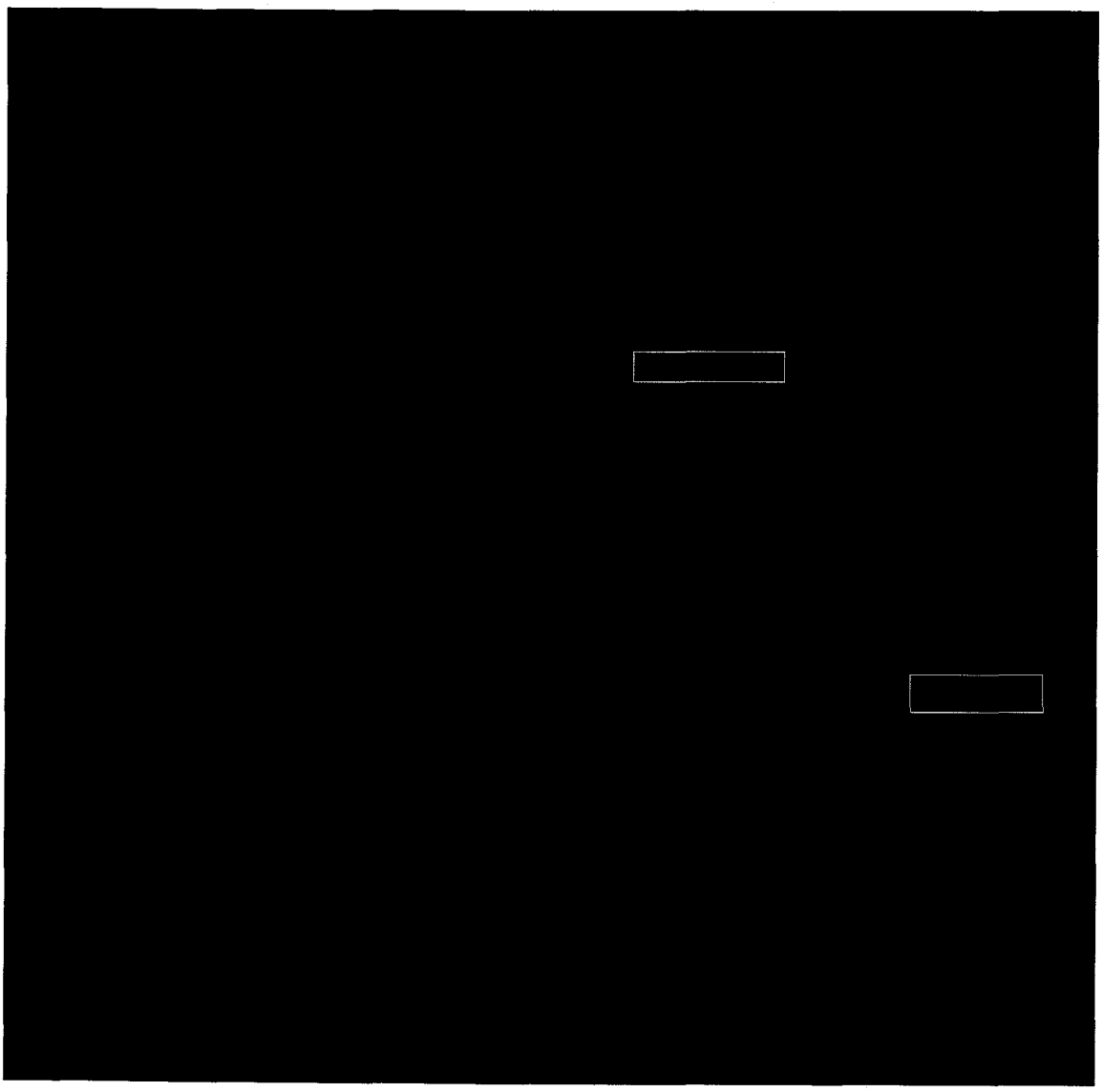
[redacted]

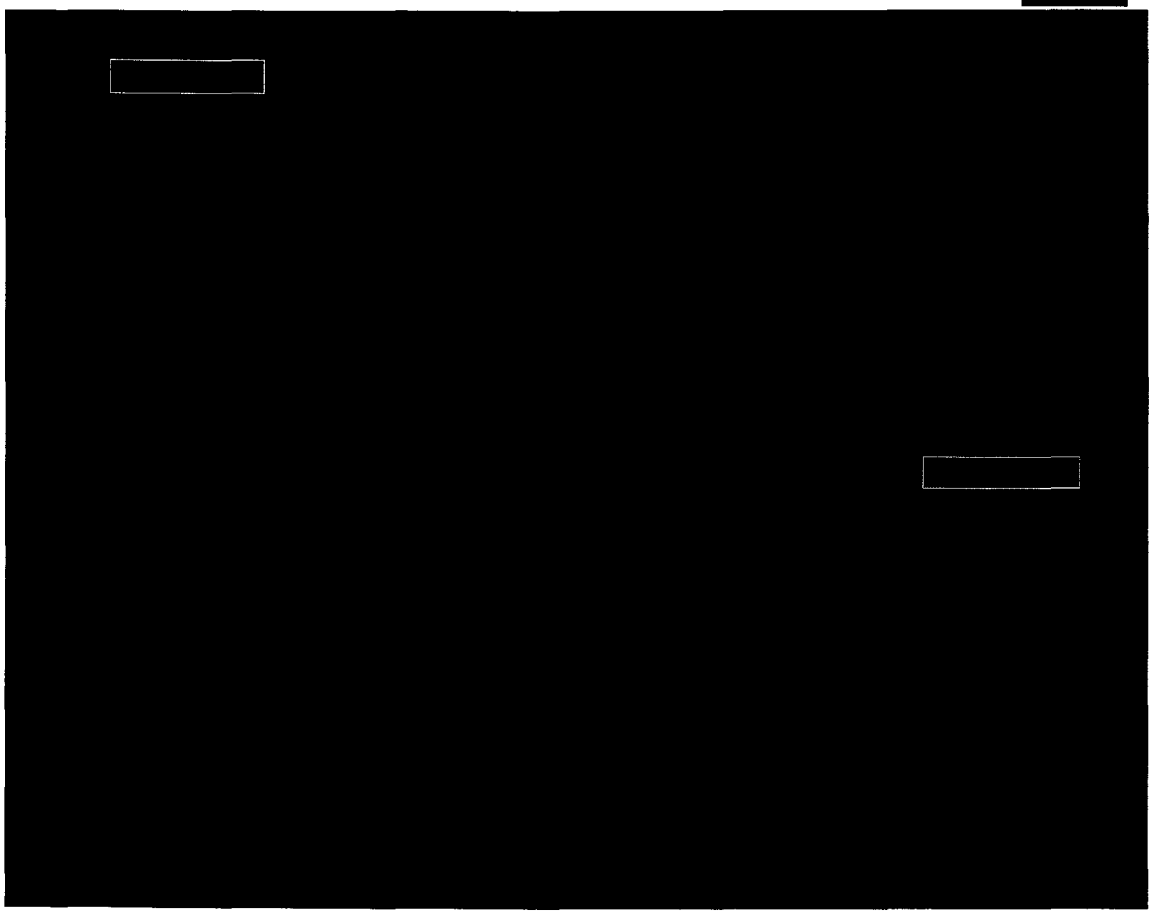
1



[redacted]

DOMESTIC EXTREMISM INTELLIGENCE REQUIREMENTS (IRs)



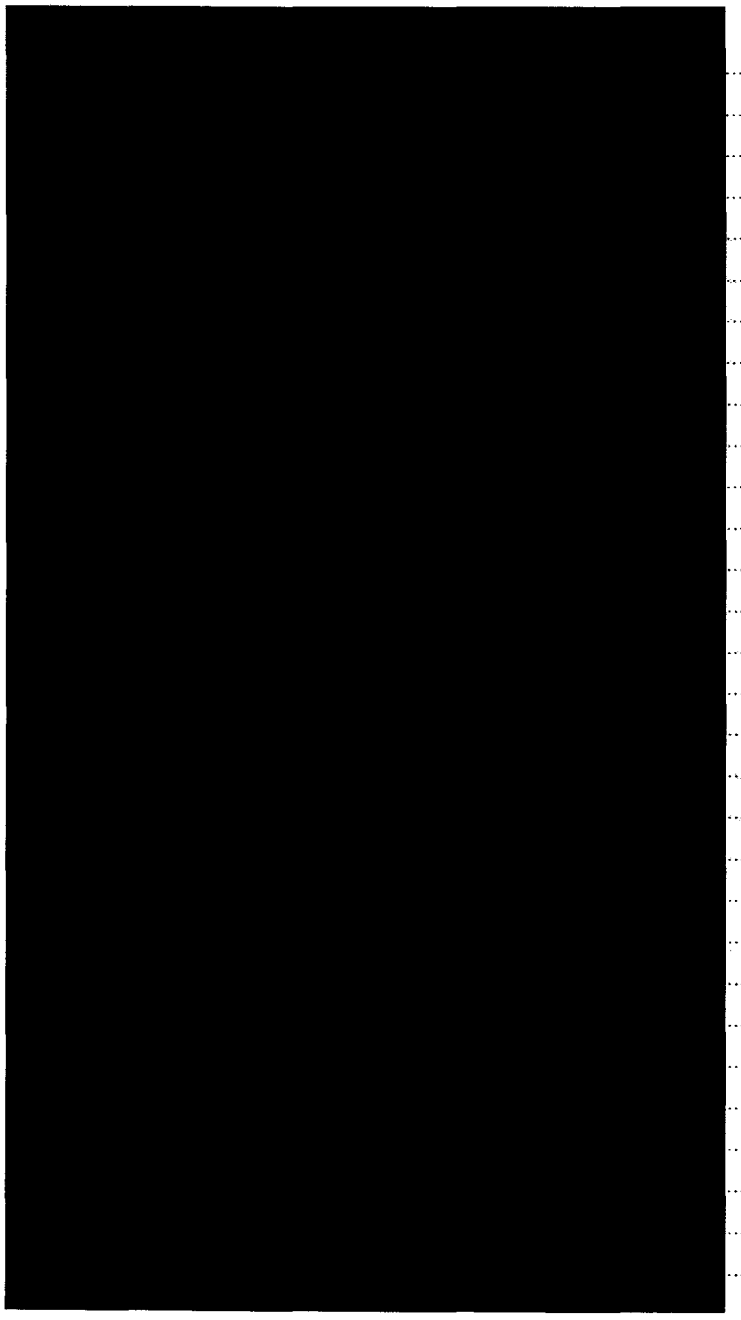


Canadian Security Intelligence Service
Intelligence Assessments

2012-2013
Intelligence Requirements

1 April 2012

[redacted]



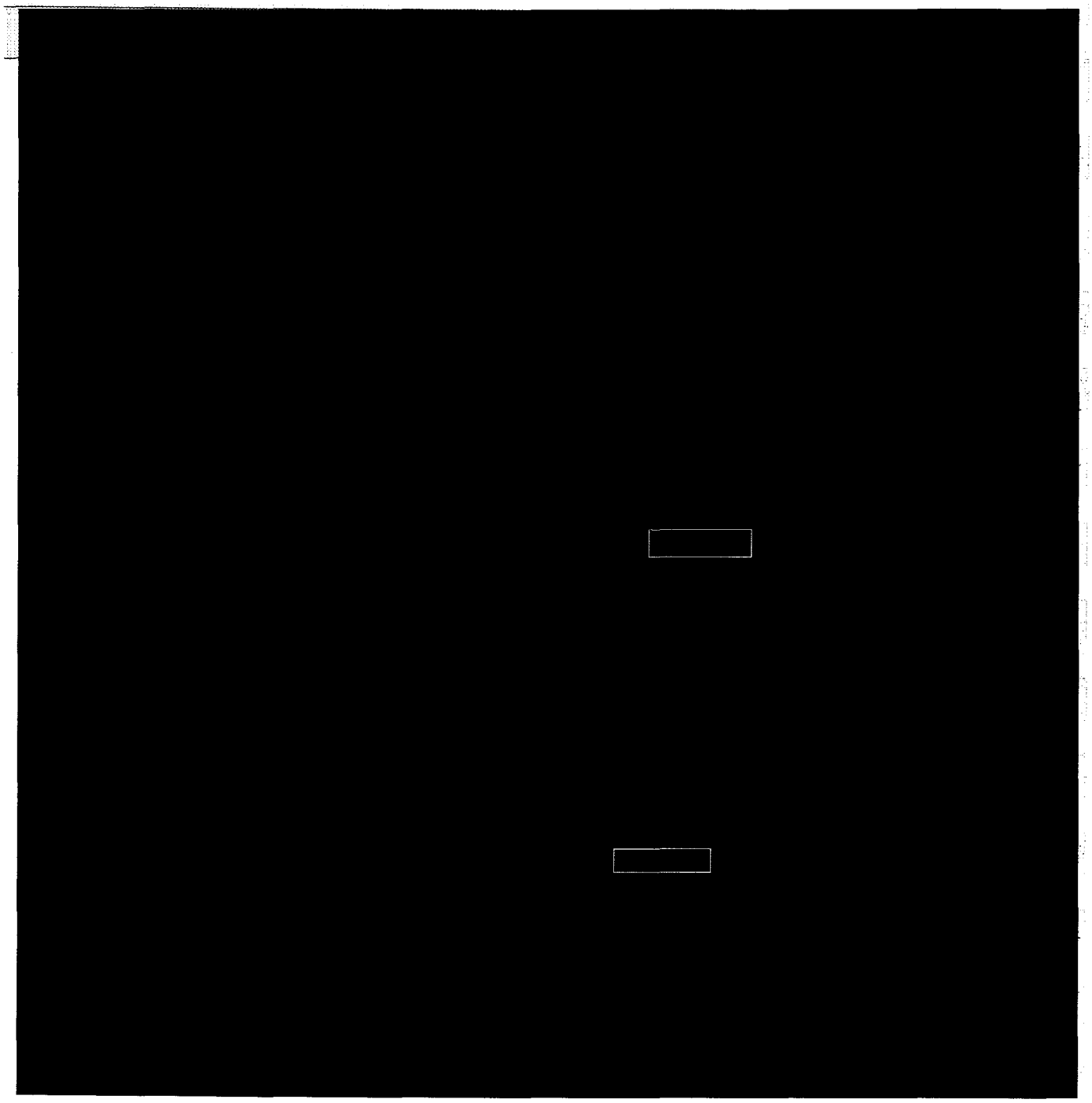
[redacted]

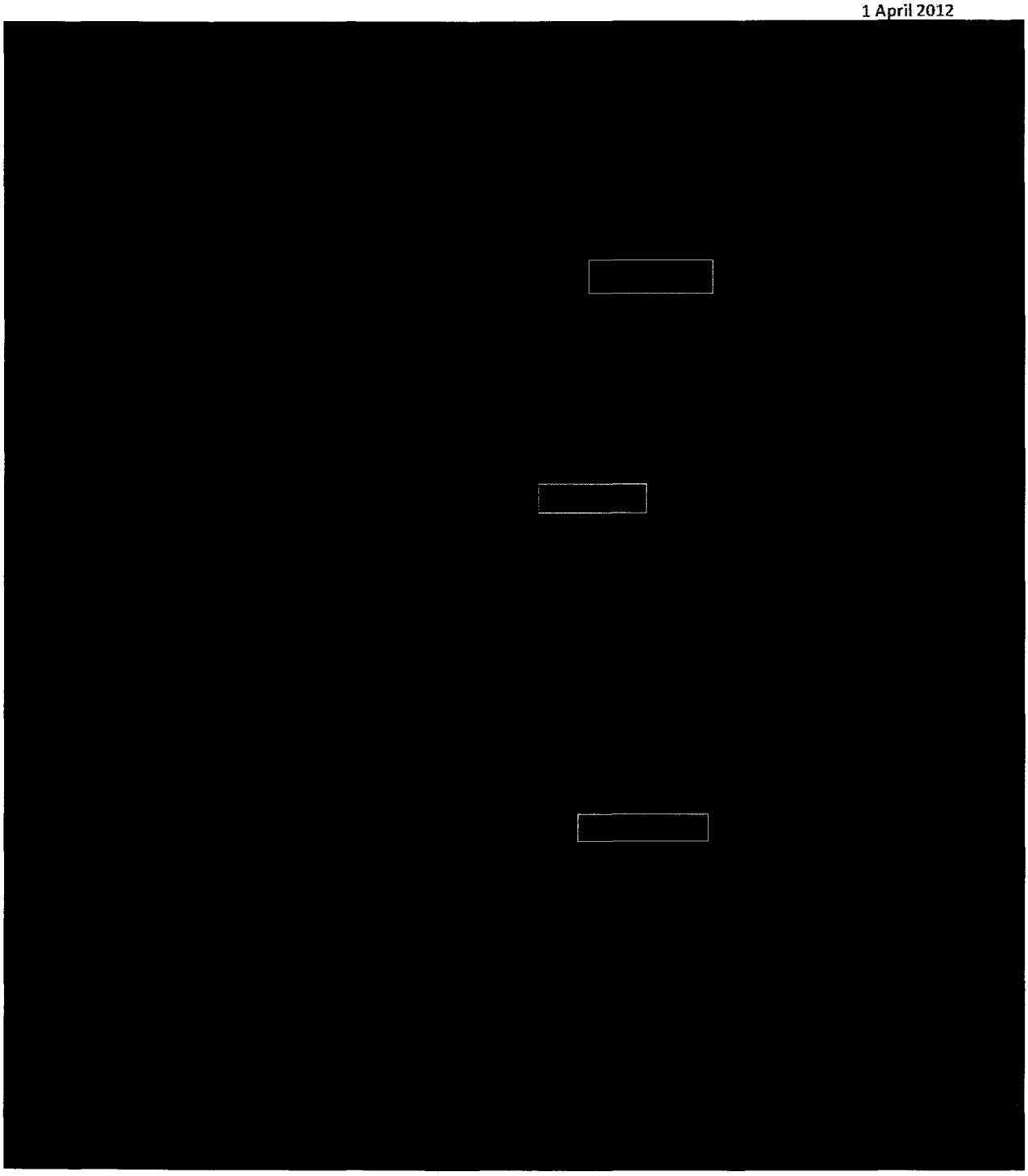
[redacted]

[redacted]

[redacted]

[redacted]





[redacted]

[redacted]

Secret CEO
[redacted]
1 April, 2015

2015-2016 INTELLIGENCE REQUIREMENTS DOCUMENT (IRD) [redacted]

[redacted]

Tab/Onglet 8

Page 604