



MAY 09 2018

CONFIDENTIAL

File: 7820-20-GNWT-151-131

MR. WILLARD HAGEN
DEPUTY MINISTER
LANDS

Access to Information and Protection of Privacy Assessment

Enclosed is the above referenced Assessment.

We will schedule a follow-up in the future to determine the progress of the agreed upon Management Action Plan. However, we would appreciate an update by August 2018 on the status of the management action plan.

We would like to thank the staff in the Department for their assistance and co-operation during the audit. Should you have any questions, please contact me at (867) 767-9175, Ext. 15215.

T. Bob Shahi
Director, Internal Audit Bureau
Finance

Enclosure

- c. Mr. Jamie Koe, Chair, Audit Committee
Ms. Brenda Hilderman, Director, Finance and Administration, Lands



LANDS

Access to Information and Protection of Privacy Assessment

Internal Audit Bureau

May 2018



LANDS

Access to Information and Protection of Privacy Assessment

May 2018

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.



CONFIDENTIAL

May 9, 2018

File: 7820-20-GNWT-151-131

MR. WILLARD HAGEN
DEPUTY MINISTER
LANDS

Audit Report: Access to Information and Protection of Privacy Assessment
Audit Period: As of March 31, 2018

A. SCOPE AND OBJECTIVES

The Audit Committee approved the GNWT wide operational audit of Access to Information and Protection of Privacy (ATIPP) legislation that focused on privacy of information.

An assessment of Lands was part of the GNWT wide audit project. This report identifies issues specific to your department.

In assessing the privacy of information for all the departments, a number of recommendations impacted more than one department. These items were reported in the "*Corporate Privacy Report*" and forwarded to the Department of Justice for further action. A copy of this report forms part of the "*Corporate Privacy Report*".

B. BACKGROUND

The 1996 *ATIPP Act* plays a critical part in maintaining government accountability and protecting the public's personal information. The legislation

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.

treats all public bodies (i.e. – departments, boards, commissions, etc.) as separate entities. The GNWT currently employs a decentralized approach where each public body has a designated access and privacy coordinator. The Department of Justice Access and Privacy Office (APO) provides government-wide support and leadership to public bodies in complying with the *ATIPP Act*.

Crowe MacKay LLP was awarded a contract through the competitive Request for Proposal process that was evaluated by staff from APO and Internal Audit Bureau (IAB).

C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

The attached audit report, *“Department of Lands, Access to Information and Protection of Privacy Act (ATIPP) Part 2”*, made a number of observations and recommendations specific to your department (**Schedule I**). The management responses to the recommendations have been incorporated in the attached report.

The contractor assessed the compliance to *ATIPP Act* and Regulations as well as nine privacy principles for your department at three levels:

- **Assessed Maturity** based on the evidence provided by your department
- **Minimum Maturity** required to be compliance to *ATIPP Act* with a target date of 12 to 24 months
- **Desired Maturity** indicates maturity that would take over 24 months to achieve.

Overall, the privacy risk for your department was assessed to be “very low” requiring internal control capacity at “ad-hoc” level. This means that that processes were primarily dependent on individuals getting things done. This was adequate capacity to meet the privacy needs of the department. Although not necessary from the risk perspective, the department could develop systematic privacy processes (repeatable level) and then focus on documenting these privacy processes (defined level). Subsequently, the department can focus on identifying and addressing privacy exceptions through monitoring (managed level). There was no compelling reason for the department to develop capacity beyond that stage (optimized level) (**Chart I refers**)

Some of the key recommendations made by the contractor were:

- Working with APO to develop and implement privacy policy
- Completing an inventory of personal information collected
- Individuals providing personal information to Lands be advised of their privacy rights.

The action plan indicated by management should address the outstanding risks. The IAB will follow-up on the status of the management action plan after six months during our scheduled follow-up audits.

D. ACKNOWLEDGEMENT

We would like to thank the department staff for their assistance and co-operation throughout the audit.



T. Bob Shahi
Director, Internal Audit Bureau
Finance

Risk and Opportunity Assessment using Capacity Model

An effective Risk Management Program balances the capacity level of internal control (people, process, and technology) with organizational risk.

		Internal Control Capacity Level				
		Ad-hoc	Repeatable	Defined	Managed	Optimized
Privacy Risk Level	Very High					
	High					
	Medium					
	Low					
	Very Low	LANDS				
		Not Compliant	Partially Compliant	Compliant	Fully Compliant	Perfectly Compliant
		Compliance Classification				

Resources used to build capacity for compliance purpose but unnecessary to address privacy risk

Risk Level and Internal Control Capacity Level are Matched.

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Scope and Objectives

The Government of the Northwest Territories (GNWT) issued a request for proposal, for an operational audit reviewing departmental compliance with Part 2 of the ACCESS to Information and Protection of Privacy Act (ATIPP or “the Act”). Crowe MacKay LLP (Crowe MacKay), being the successful proponent. The work was coordinated directly under the supervision of the Director, Internal Audit Bureau.

Testing of departments was based on the Generally Accepted Privacy Principles (GAPP) which incorporates 10 principles, each backed up by an objective and measurable criteria to determine risk and compliance within each department included in our scope. We reviewed key controls related to each of the principles, taking into account their associated criteria. This testing was conducted on current approaches to and compliance activities of each department.

Preliminary survey determined that the maturity of GNWT’s control environment related to Part 2: Protection of Privacy was less mature than that related to Part 1: Access to Information. Considering the less mature control environment likely in place for most departments, the focus of the audit was adjusted to be less compliance-based and more risk-based with a strong focus on the maturity levels denoted in the AICPA/CICA Privacy Maturity Model (Privacy Maturity Model) (Appendix A refers). We relied less on substantive testing of controls already in place and addressed the risks related to effectively establish a sound governance framework by the Access and Privacy Office as well as how each department interpreted this framework for departmental application. With regards to the integrity of information held in the custody of each department, the compilation of that personal information and the thought/opinions provided by each department of their control environment for appropriately protecting this personal information, this audit assessed what was being done in order to gain comfort and provide support for the opinions of each department where possible.

Departmental Background

The Department of Lands (“Lands”) was created in April 2014, transferring public land management and administration functions from the federal government for Territorial lands and from the GNWT Department of Municipal and Community Affairs for Commissioner’s Lands. Lands meets its responsibilities through programs it offers through its divisions of:

- Directorate;
- Finance and Administration;
- Informatics Shared Services;
- Commissioner’s and Territorial Land Administration;
- Land Use and Sustainability;
- Policy, Legislation and Communications;
- Regional offices; and
- Securities and Project Assessment.

Lands collects personal information through:

- Commissioner’s and Territorial Land Administration
- Informatics Shared Services Centre

Personal information collected as part of Land Administration is stored in the LIMS database – Lands Lease Information Management System, LAS – Commissioner’s Lands Lease Administration System, IRRA – Inspection Risk Reporting Analysis program, and ATLAS (Administration of the Territorial Land Acts System).

The NWT Centre for Geomatics in the Informatics Shared Services Centre collects names, addresses and email information from users wishing to download geospatial information from their website as some

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

datasets are under a specific license agreement. This information is stored in an MS SQL database which has restricted access to three individuals.

All divisions store information collected in hard copy under the Operational Records Classification System and the Administrative Records Classification System, including electronic information in the Digital Integrated Information Management System (DIIMs).

Overview

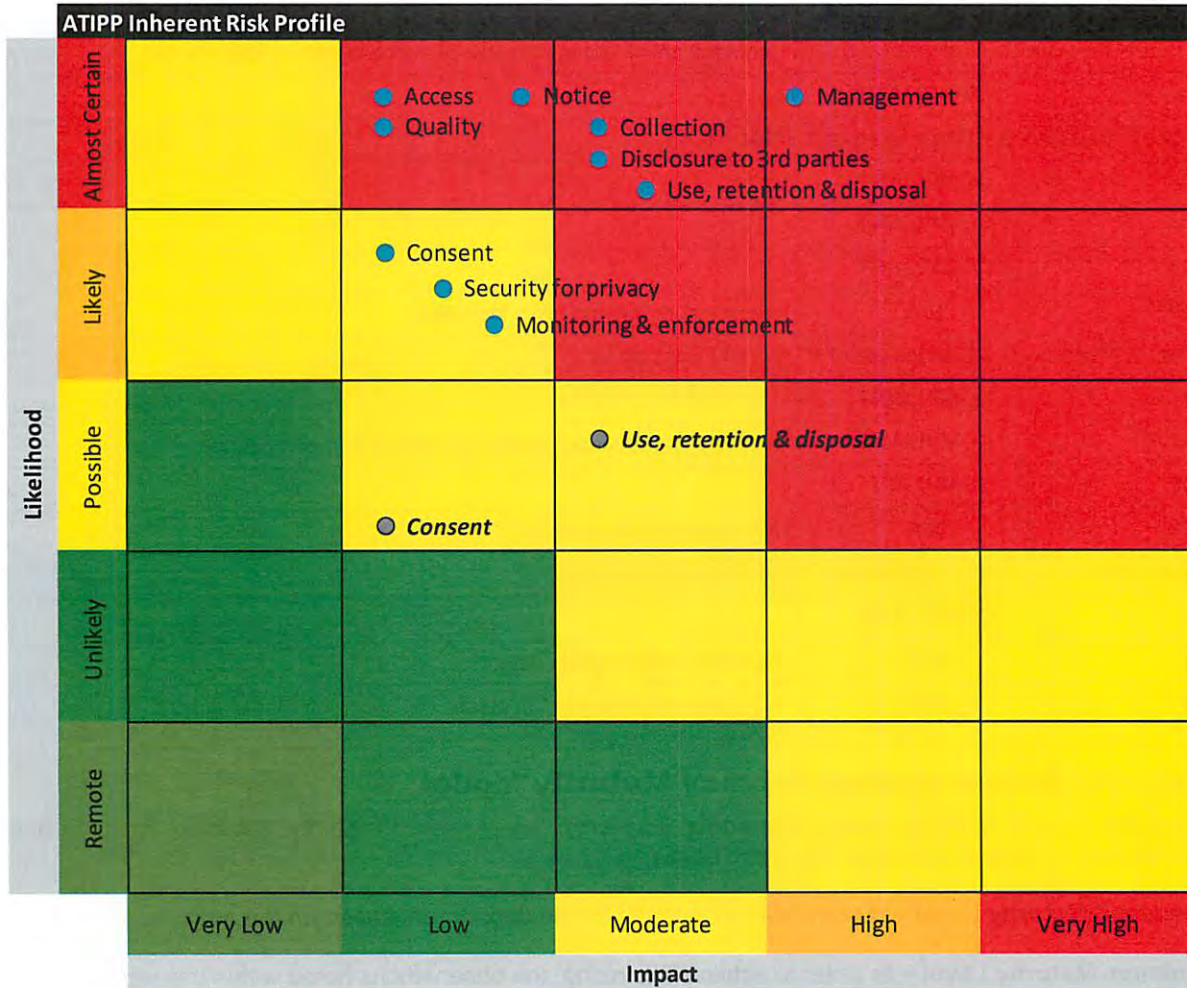
Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP Coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. The heatmap shows the initial inherent risk rating for each principle in regular black print as well as our applied rating based on the results of our department review in bold italics. Changes represent recognition of controls implemented by the department which serve to reduce risk. For example, a rating of ad hoc in relation to a principle area would result in no change in the risk map as no controls have yet been implemented rating higher in the maturity model will result in an adjustment to the heat map placement and an entry in the new locations denoted by bold and italics.

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

RISK HEATMAP



Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

Based on the audit work performed the department is not fully compliant with ATIPP Part 2. Support for this is as follows:

Section	Compliance Assessment	Reason for Non-Compliance
Part 2: Division A – Collection of Personal Information		
40	COMPLIANT	
41 (1)	COMPLIANT	

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Section	Compliance Assessment	Reason for Non-Compliance
41 (2) & (3)	NOT COMPLIANT	Legal authority for collection of information and contact information is not provided on all forms. Principle of notice is not completely met.
42	COMPLIANT	
Part 2: Division B – Use of Personal Information		
43	COMPLIANT	
44	COMPLIANT	
45	COMPLIANT	
46	N/A	A disclosure has not been identified.
Part 2: Division C – Disclosure of Personal Information		
47	COMPLIANT	
47.1	COMPLIANT	No reporting received to date to indicate non-compliance.
48	COMPLIANT	
49	N/A	No research use identified
Regulations relating to disclosure of personal information		
5	COMPLIANT	
6	N/A	No formal examination noted.
8	N/A	No research agreement in place.

Maturity Rating against Privacy Maturity Model

Using the Privacy Maturity Model (**Appendix A refers**), the assessed maturity, minimum maturity and desired maturity are illustrated in the graph below.

Assessed Maturity Level – current level of maturity for the department based on the audit.

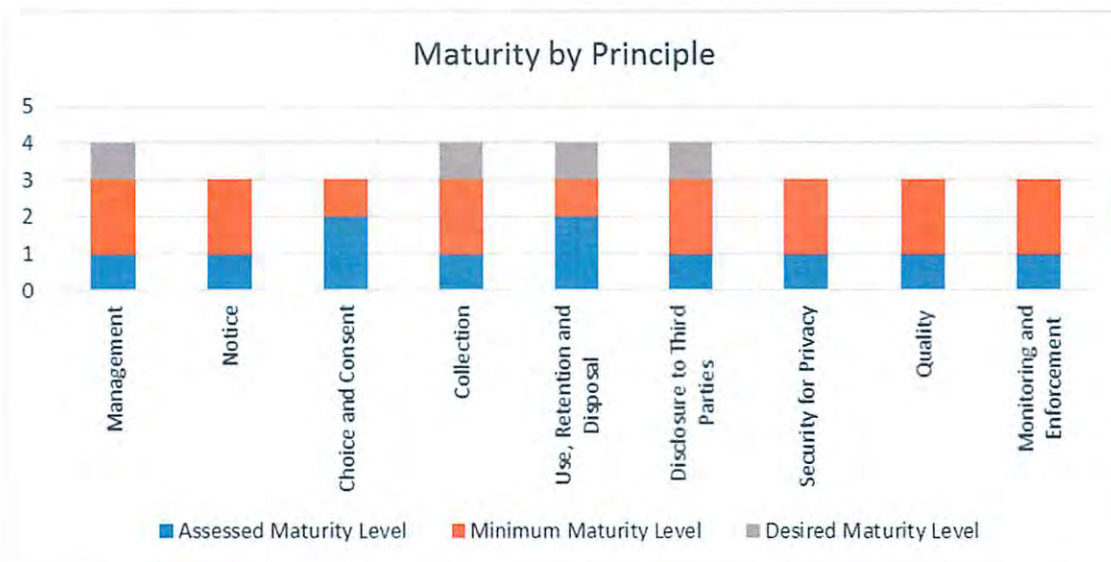
Minimum Maturity Level – In order to achieve this rating, the observations noted within this report must be addressed (short term timeframe 12-24 months).

Desired Maturity Level – This level would be achieved via long term goals (>24 months) and should be part of long term planning if applicable to your department.

Please note that departments with data which has been assessed as lower risk are only required to reach the minimum maturity level. As Lands does not deal with higher risk data, this department is expected to work towards the minimum maturity level set out below.

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)



Overall findings, including rating of the department against each privacy principle, is summarized in the following table:

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p>Management</p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Ad Hoc	<ul style="list-style-type: none"> Privacy policies have not been formally designed and documented. An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved. There is a strong departmental culture over personal information through informal communications. An ATIPP Coordinator has been assigned. ATIPP Coordinator has been waiting to take the training sessions offered by the Privacy Office. Privacy Impact Assessments do not appear to be used at this time <p><i>See observations 1-3.</i></p>
<p>Notice</p> <p>The department provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.</p>	Ad Hoc	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address notice to individuals. Notice is not provided on all forms used to collect personal information. <p><i>See observation 4.</i></p>
<p>Consent</p> <p>The department describes the choices available to the individual and obtains implicit or explicit consent with respect</p>	Repeatable	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address consent of individuals.

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
to the collection, use and disclosure of personal information.		<ul style="list-style-type: none"> • Implicit consent is obtained on personal information collection forms. • Explicit consent is obtained on information collection forms. <p><i>See observation 1.</i></p>
<p>Collection</p> <p>The department collects personal information only for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address collection of personal information. • The type of personal information collected and the method of collection for personal information collected by forms is known to the individual. • Personal information is not collected by third parties. • Methods and forms of collecting information are not provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means. • A procedure/process does not exist to ensure only information needed is collected. <p><i>See observations 5-6.</i></p>
<p>Use, retention and disposal</p> <p>The department limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.</p>	Repeatable	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address use, retention and disposal. • There are security provisions in place to ensure that data cannot be pulled and used for purposes other than that for which it was collected, but there are no documented processes in place to ensure information collected is only used for the purpose for which it was collected • Retention and disposal of information is outlined in the Operational Records Classification System and the Administrative Records Classification System schedules and in the Digital Integrated Information Management System (DIIMs) which allows for information to be retained for no longer than necessary and is disposed of at that time. <p><i>See observation 5.</i></p>
<p>Disclosure to third parties</p> <p>The department discloses personal information to third parties only for the purposes identified in the notice and</p>	Ad Hoc	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address disclosure to third parties and what remedial action should be

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
with the implicit or explicit consent of the individual.		<p>taken if the information was misused by the third party.</p> <ul style="list-style-type: none"> Information sharing agreements do not exist with other departments to provide instructions or requirements to the departments regarding the personal information disclosed, to ensure the information is only used for the purpose for which it was collected and to ensure the information will be protected in a manner consistent the department's requirements. Policy exists that provides guidance on how to address requests for lease information from lenders. <p><i>See observation 7.</i></p>
<p>Security for privacy</p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented. Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place by the Informatics Shared Services Centre. Physical access to personal information is restricted through access to building, floor restriction access, storage in secure and locked cabinets. Security measures exist over the transmission of data but are not formally designed and documented. Tests of all safeguards in place are not performed. <p><i>See observation 1.</i></p>
<p>Quality</p> <p>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address quality to ensure personal information is complete and accurate for the purposes for which it is to be used and it is relevant to the purposes for which it is to be used. <p><i>See observation 1.</i></p>
<p>Monitoring and enforcement</p> <p>The department monitors compliance with its privacy policies and procedures and has procedures to address</p>	Ad Hoc	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address monitoring and enforcement. Monitoring and enforcement are not being done at present.

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
privacy-related complaints and disputes.		See observation 1.

Observations and Recommendations

Observation 1

Privacy policy has not been designed and documented

- When the department was created in 2014 the policies and procedures of the federal and territorial functions assumed were adopted, which did not include specific privacy policies.
- The policies have not been reviewed nor updated since the department was created in regards to privacy, specifically ATIPP part 2.

Risk Profile:

Risk Impact	Without a documented privacy policy, consistent direction cannot be given to departmental personnel which results in inconsistent or non-compliance with ATIPP legislation.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

Recommendations:

We recommend that:

- The Department of Justice develop a GNWT-wide privacy policy and associated guidelines.
- The department should work with Justice to ensure that departmental processes and procedures are set up to allow the department to meet the overarching policy and guidelines.
- This one policy should address requirements as set out within the ATIPP Act, and ensure the privacy principles are sufficiently addressed to meet minimum maturity requirements.

Management Response:

Action Plan	Completion Date:
<p>The Department of Justice is in the process of developing a GNWT-wide Protection of Privacy Policy. The draft Policy has been shared with all departments for review and discussion. It is anticipated that the Policy will be finalized by June 30, 2018.</p> <p>The draft Protection of Privacy Policy is part of an overarching GNWT Privacy Framework that is being developed to support departments in ensuring that the privacy provisions of the ATIPP Act are administered in a consistent and fair manner. The framework will include guidelines to assist departments in developing their own privacy management programs. The Department of Justice anticipates finalizing the Privacy</p>	December 2018

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Framework by June 30, 2018 and will be working with departments to implement the framework across the GNWT over the summer/fall of 2018.	
--	--

Observation 2

An inventory of personal information collected does not exist

- Department staff have knowledge of the personal information collected by their division but it is not documented and a global listing cannot be readily created or obtained.
- Systems involved in collection and storage of personal information are not documented.
- Third parties involved are not documented.

Risk Profile:

Risk Impact	Without an inventory of personal information, it is not possible for the department to ensure that all areas containing personal information are correctly protected under ATIPP.
Risk Responsibility	All Divisional directors/Superintendents and the ATIPP Coordinator
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

Recommendations:

We recommend that:

- An inventory of the types of personal information and the related processes, systems, and third parties involved be created by each division and be submitted to the ATIPP Coordinator for consolidation into a global department inventory. A review of all areas should then take place to ensure compliance processes and procedures are in place.

Management Response:

Action Plan	Completion Date:
The Department will develop a global inventory of all the types of personal information and the related processes and systems. Each divisional director will be responsible to provide the information to the ATIPP Coordinator.	October 2018
Once the new GNWT Privacy Management Program is in place and the Department has the tools and guidelines it needs, the ATIPP Coordinator will conduct an internal review to ensure compliance processes and procedures are in place.	March 2019

Observation 3

There is a lack of support provided to ATIPP within the Department

- ATIPP Coordinator has not been able to take the three-day in-depth ATIPP training by the Privacy Office; currently the knowledge level is inadequate to allow this individual to effectively complete their full ATIPP responsibilities.

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

- Job description of the ATIPP Coordinator, who is also the Director, Policy, Legislation and Communications outlines responsibilities for only Part 1 of ATIPP responsibilities and not Part 2.

Risk Profile:

Risk Impact	Without a set role with assigned responsibilities as outlined in a job description, the privacy function (whether part of another role or in its own capacity) will be limited in ability to fulfill the role. Without additional avenues for training, there is increased risk that the privacy Coordinator may not have the full understanding required to carry out the role.
Risk Responsibility	Deputy Minister and Assistant Deputy Minister Planning and Coordination
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

Recommendations:

We recommend that:

- The roles and responsibilities of the ATIPP Coordinator be defined, addressing both ATIPP Part 1 and Part 2
- Training for ATIPP Coordinator be reviewed and adjusted as needed to ensure that there is both awareness and understanding of the full responsibilities of ATIPP compliance. This will allow for better provision of guidance to the department.
- The department should evaluate capacity and capability of current resources. Awareness of resources for ATIPP understanding, training and guidance is required along with support for ATIPP compliance activities.

Management Response:

Action Plan	Completion Date:
The Job Description for the Director, Policy Legislation and Communications position will be amended to include responsibilities under Part 1 and Part 2 of the ATIPP Act and reevaluated by HR.	July 2018

Observation 4

Forms used to collect personal information are not consistently providing the required notice

- Notice regarding consent, collection, use, retention and disposal, third party disclosure, security protection, quality and monitoring and enforcement is missing from forms were used for GNWT functions prior to the creation of Lands.
- The department is not compliant with ATIPP Part 2 legislation because of the lack of notice provided specifically related to individuals being informed about how to contact the entity with inquiries, complaints and disputes.
- Forms used for functions that were Federal government functions prior to the creation of Lands contain the required notice.

Risk Profile:

Risk Impact	Lack of notice on forms will result in the department not being compliant with ATIPP legislation.
Risk Responsibility	Director Commissioner's Land Administration

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office
-------------------------	---

Recommendations:

We recommend that:

- All forms used to collect personal information be reviewed and updated to consistently provide the required notice to individuals.

Management Response:

Action Plan	Completion Date:
The Department will review and amend the Application Forms for Commissioner's Land to include the privacy notice and ensure that the forms are compliant with Part 2 of the ATIPP Act.	May 2018

Observation 5

Methods of collection are not reviewed by ATIPP Coordinator prior to implementation

- New collection methods are not reviewed to ensure they are fair and lawful.
- New collection methods are not reviewed to ensure only information needed for its purpose is being collected. A privacy impact assessment is not performed.

Risk Profile:

Risk Impact	Without a review of collection methods being introduced, there is an increased risk of non-compliance with ATIPP legislation during these new collection methods.
Risk Responsibility	Delegated ATIPP Coordinator and all Divisional Directors/Superintendents
Risk Mitigation Support	The office of the GNWT Access and Privacy Office

Recommendations:

We recommend that:

- A procedure be formalized that requires all new methods of information collection to be reviewed and approved by the ATIPP Coordinator.
- A procedure be formalized which specifies actions to be taken by the ATIPP Coordinator to validate only information needed is collected through fair and lawful means.
- A privacy impact assessment should be performed for all new information collection methods or changes to existing methods.

Management Response:

Action Plan	Completion Date:
Once the new GNWT Privacy Management Program is in place and the Department has the tools and guidelines it needs, the ATIPP Coordinator will develop a directive/procedure for all Divisions to submit any new method of information collection for review and assessment. The directive will include the requirement for all divisions to conduct a privacy impact assessment as part of the package to be	March 2019

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

reviewed.	
-----------	--

Observation 6

Procedures do not exist to ensure only information needed is collected

- Existing methods of collection are not reviewed by the ATIPP Coordinator along with key stakeholders as required to ensure only information needed is being collected.

Risk Profile:

Risk Impact	If additional information is collected beyond that required by the use for which disclosure was made to the individual, the department will not be in compliance with ATIPP legislation
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

Recommendations:

We recommend that:

- The department reevaluate and reassess the current information collection needs to support the department mandate.
- The personal information essential for the collection purpose be clearly documented and distinguished from optional information for each program for which personal information collection is required.
- Existing forms be reviewed against documented personal information essential for use and changed as necessary to collect only the information required for the purpose for which it's being collected.

Management Response:

Action Plan	Completion Date:
Once the new GNWT Privacy Management Program is in place and the Department has the tools and guidelines it needs, the Director of Commissioner's Land Administration and the Director of Territorial Land Administration will review and reevaluate the information that is being collected to ensure that only essential information is being collected. Based on the review, the application forms will be amended accordingly, if necessary.	March 2019
The NWT Genomatics Centre is currently reviewing the need to collect personal information from users that download geospatial datasets	October 2018

Observation 7

Information sharing agreements do not exist between LANDS and other GNWT departments

- A listing does not exist which details the type of information shared through information sharing agreements, with which departments and for what use.

DEPARTMENT OF LANDS

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Risk Profile:

Risk Impact	When information sharing agreements are not in place there is increased risk that proper disclosures are not made to the owners of the personal information being shared.
Risk Responsibility	Assistant Deputy Minister Operations, Executive Director Informatics Shared Services Centre, and Director Finance and Administration
Risk Mitigation Support	All Divisional Directors, the Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

Recommendations:

We recommend that:

- A listing of all information provided to other departments be compiled which details what information is provided, to which department and for what use and that the listing be reviewed to assess whether the information shared is required to be shared.
- Information sharing agreements be entered into with departments that receive necessary personal information from LANDS and that the agreements provide instructions or requirements regarding the personal information disclosed to ensure the information is only used for the purpose for which it was collected and to ensure the information will be protected in a manner consistent the department's requirements.

Management Response:

Action Plan	Completion Date:
The Department will develop a listing of all the private information that is shared with other GNWT Departments, and review its necessity for being shared.	October 2018
Once the new GNWT Privacy Management Program is in place and the Department has the tools and guidelines it needs, the Department will draft and enter into information sharing agreements with the other GNWT departments.	March 2019

Responses provided by Shauna Hamilton with copies to Brenda Hilderman, Shelly Kavanagh and Kate Hearn.

AICPA/CICA Privacy Maturity Model

March 2011



Appendix A

Notice to Reader

DISCLAIMER: This document has not been approved, disapproved, or otherwise acted upon by any senior technical committees of, and does not represent an official position of the American Institute of Certified Public Accountants (AICPA) or the Canadian Institute of Chartered Accountants (CICA). It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services in this document. The services of a competent professional should be sought when legal advice or other expert assistance is required.

Neither the authors, the publishers nor any person involved in the preparation of this document accept any contractual, tortious or other form of liability for its contents or for any consequences arising from its use. This document is provided for suggested best practices and is not a substitute for legal advice. Obtain legal advice in each particular situation to ensure compliance with applicable laws and regulations and to ensure that procedures and policies are current as legislation and regulations may be amended.

Copyright©2011 by
American Institute of Certified Public Accountants, Inc.
and Canadian Institute of Chartered Accountants.

All rights reserved. Checklists and sample documents contained herein may be reproduced and distributed as part of professional services or within the context of professional practice, provided that reproduced materials are not in any way directly offered for sale or profit. For information about the procedure for requesting permission to make copies of any part of this work, please visit www.copyright.com or call (978) 750-8400.

AICPA/CICA Privacy Task Force

Chair

Everett C. Johnson, CPA

Vice Chair

Kenneth D. Askelson, CPA, CITP, CIA

Eric Federing

Philip M. Juravel, CPA, CITP

Sagi Leizerov, Ph.D., CIPP

Rena Mears, CPA, CITP, CISSP, CISA, CIPP

Robert Parker, FCA, CA•CISA, CMC

Marilyn Prosch, Ph.D., CIPP

Doron M. Rotman, CPA (Israel), CISA, CIA, CISM, CIPP

Kerry Shackelford, CPA

Donald E. Sheehy, CA•CISA, CIPP/C

Staff Contacts:

Nicholas F. Cheung, CA, CIPP/C

CICA

Principal, Guidance and Support

and

Nancy A. Cohen, CPA, CITP, CIPP

AICPA

Senior Technical Manager, Specialized Communities and Practice Management

Appendix A

AICPA/CICA Privacy Maturity Model

Acknowledgements

The AICPA and CICA appreciate the contributions of the volunteers who devoted significant time and effort to this project. The institutes also acknowledge the support that the following organization has provided to the development of the Privacy Maturity Model:



Table of Contents

1 Introduction	1
2 AICPA/CICA Privacy Resources	1
Generally Accepted Privacy Principles (GAPP)	1
Privacy Maturity Model	2
3 Advantages of Using the Privacy Maturity Model	2
4 Using the Privacy Maturity Model	2
Getting Started	3
Document Findings against GAPP	3
Assessing Maturity Using the PMM	3
5 Privacy Maturity Model Reporting	3
6 Summary	4
AICPA/CICA PRIVACY MATURITY MODEL	
Based on Generally Accepted Privacy Principles (GAPP)	5

Appendix A

AICPA/CICA Privacy Maturity Model

This page intentionally left blank.

AICPA/CICA Privacy Maturity Model User Guide

1 INTRODUCTION

Privacy related considerations are significant business requirements that must be addressed by organizations that collect, use, retain and disclose personal information about customers, employees and others about whom they have such information. **Personal information** is information that is about, or can be related to, an identifiable individual, such as name, date of birth, home address, home telephone number or an employee number. Personal information also includes medical information, physical features, behaviour and other traits.

Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.

Becoming privacy compliant is a journey. Legislation and regulations continue to evolve resulting in increasing restrictions and expectations being placed on employers, management and boards of directors. Measuring progress along the journey is often difficult and establishing goals, objectives, timelines and measurable criteria can be challenging. However, establishing appropriate and recognized benchmarks, then monitoring progress against them, can ensure the organization's privacy compliance is properly focused.

2 AICPA/CICA PRIVACY RESOURCES

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have developed tools, processes and guidance based on **Generally Accepted Privacy Principles (GAPP)** to assist organizations in strengthening their privacy policies, procedures and practices. GAPP and other tools and guidance such as the AICPA/CICA Privacy Risk Assessment Tool, are available at www.aicpa.org/privacy and www.cica.ca/privacy.

Generally Accepted Privacy Principles (GAPP)

Generally Accepted Privacy Principles has been developed from a business perspective, referencing some but by no means all significant local, national and international privacy regulations. GAPP converts complex privacy requirements into a single privacy objective supported by 10 privacy principles. Each principle is supported by objective, measurable criteria (73 in all) that form the basis for effective management of privacy risk and compliance. Illustrative policy requirements, communications and controls, including their monitoring, are provided as support for the criteria.

GAPP can be used by any organization as part of its privacy program. GAPP has been developed to help management create an effective privacy program that addresses privacy risks and obligations as well as business opportunities. It can also be a useful tool to boards and others charged with governance and the provision of oversight. It includes a definition of privacy and an explanation of why privacy is a business issue and not solely a compliance issue. Also illustrated are how these principles can be applied to outsourcing arrangements and the types of privacy initiatives that can be undertaken for the benefit of organizations, their customers and related persons.

The ten principles that comprise GAPP:

- **Management.** The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
- **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
- **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
- **Collection.** The entity collects personal information only for the purposes identified in the notice.
- **Use, retention and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
- **Access.** The entity provides individuals with access to their personal information for review and update.
- **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

- **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
- **Quality.** The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.
- **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Since GAPP forms the basis for the Privacy Maturity Model (PMM), an understanding of GAPP is required. In addition, an understanding of the entity's privacy program and any specific privacy initiatives is also required. The reviewer should also be familiar with the privacy environment in which the entity operates, including legislative, regulatory, industry and other jurisdictional privacy requirements.

Privacy Maturity Model

Maturity models are a recognized means by which organizations can measure their progress against established benchmarks. As such, they recognize that:

- becoming compliant is a journey and progress along the way strengthens the organization, whether or not the organization has achieved all of the requirements;
- in certain cases, such as security-focused maturity models, not every organization, or every security application, needs to be at the maximum for the organization to achieve an acceptable level of security; and
- creation of values or benefits may be possible if they achieve a higher maturity level.

The AICPA/CICA Privacy Maturity Model¹ is based on GAPP and the Capability Maturity Model (CMM) which has been in use for almost 20 years.

The PMM uses five maturity levels as follows:

1. Ad hoc – procedures or processes are generally informal, incomplete, and inconsistently applied.
2. Repeatable – procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.

¹ This model is based on Technical Report, CMU/SEI-93TR-024 ESC-TR-93-177, "Capability Maturity Model SM for Software, Version 1.1," Copyright 1993 Carnegie Mellon University, with special permission from the Software Engineering Institute. Any material of Carnegie Mellon University and/or its Software Engineering Institute contained herein is furnished on an "as-is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement. This model has not been reviewed nor is it endorsed by Carnegie Mellon University or its Software Engineering Institute. Capability Maturity Model, CMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

3. Defined – procedures and processes are fully documented and implemented, and cover all relevant aspects.
4. Managed – reviews are conducted to assess the effectiveness of the controls in place.
5. Optimized – regular review and feedback are used to ensure continuous improvement towards optimization of the given process.

In developing the PMM, it was recognized that each organization's personal information privacy practices may be at various levels, whether due to legislative requirements, corporate policies or the status of the organization's privacy initiatives. It was also recognized that, based on an organization's approach to risk, not all privacy initiatives would need to reach the highest level on the maturity model.

Each of the 73 GAPP criteria is broken down according to the five maturity levels. This allows entities to obtain a picture of their privacy program or initiatives both in terms of their status and, through successive reviews, their progress.

3 ADVANTAGES OF USING THE PRIVACY MATURITY MODEL

The PMM provides entities with a useful and effective means of assessing their privacy program against a recognized maturity model and has the added advantage of identifying the next steps required to move the privacy program ahead. The PMM can also measure progress against both internal and external benchmarks. Further, it can be used to measure the progress of both specific projects and the entity's overall privacy initiative.

4 USING THE PRIVACY MATURITY MODEL

The PMM can be used to provide:

- the status of privacy initiatives
- a comparison of the organization's privacy program among business or geographical units, or the enterprise as a whole
- a time series analysis for management
- a basis for benchmarking to other comparable entities.

To be effective, users of the PMM must consider the following:

- maturity of the entity's privacy program
- ability to obtain complete and accurate information on the entity's privacy initiatives
- agreement on the Privacy Maturity assessment criteria
- level of understanding of GAPP and the PMM.

Getting Started

While the PMM can be used to set benchmarks for organizations establishing a privacy program, it is designed to be used by organizations that have an existing privacy function and some components of a privacy program. The PMM provides structured means to assist in identifying and documenting current privacy initiatives, determining status and assessing it against the PMM criteria.

Start-up activities could include:

- identifying a project sponsor (Chief Privacy Officer or equivalent)
- appointing a project lead with sufficient privacy knowledge and authority to manage the project and assess the findings
- forming an oversight committee that includes representatives from legal, human resources, risk management, internal audit, information technology and the privacy office
- considering whether the committee requires outside privacy expertise
- assembling a team to obtain and document information and perform the initial assessment of the maturity level
- managing the project by providing status reports and the opportunity to meet and assess overall progress
- providing a means to ensure that identifiable risk and compliance issues are appropriately escalated
- ensuring the project sponsor and senior management are aware of all findings
- identifying the desired maturity level by principle and/or for the entire organization for benchmarking purposes.

Document Findings against GAPP

The maturity of the organization's privacy program can be assessed when findings are:

- documented and evaluated under each of the 73 GAPP criteria
- reviewed with those responsible for their accuracy and completeness
- reflective of the current status of the entity's privacy initiatives and program. Any plans to implement additional privacy activities and initiatives should be captured on a separate document for use in the final report.

As information on the status of the entity's privacy program is documented for each of the 73 privacy criteria, it should be reviewed with the providers of the information and, once confirmed, reviewed with the project committee.

Assessing Maturity Using the PMM

Once information on the status of the entity's privacy program has been determined, the next task is to assess that information against the PMM.

Users of the PMM should review the descriptions of the activities, documents, policies, procedures and other information expected for each level of maturity and compare them to the status of the organization's privacy initiatives.

In addition, users should review the next-higher classification and determine whether the entity could or should strive to reach it.

It should be recognized that an organization may decide for a number of reasons not to be at maturity level 5. In many cases a lower level of maturity will suffice. Each organization needs to determine the maturity level that best meets their needs, according to its circumstances and the relevant legislation.

Once the maturity level for each criterion has been determined, the organization may wish to summarize the findings by calculating an overall maturity score by principle and one for the entire organization. In developing such a score, the organization should consider the following:

- sufficiency of a simple mathematical average; if insufficient, determination of the weightings to be given to the various criteria
- documentation of the rationale for weighting each criterion for use in future benchmarking.

5 PRIVACY MATURITY MODEL REPORTING

The PMM can be used as the basis for reporting on the status of the entity's privacy program and initiatives. It provides a means of reporting status and, if assessed over time, reporting progress made.

In addition, by documenting requirements of the next-higher level on the PMM, entities can determine whether and when they should initiate new privacy projects to raise their maturity level. Further, the PMM can identify situations where the maturity level has fallen and identify opportunities and requirements for remedial action.

Privacy maturity reports can be in narrative form; a more visual form can be developed using graphs and charts to indicate the level of maturity at the principle or criterion level.

The following examples based on internal reports intended for management use graphical representations.

Figure 1 - Privacy Maturity Report by GAPP Principle

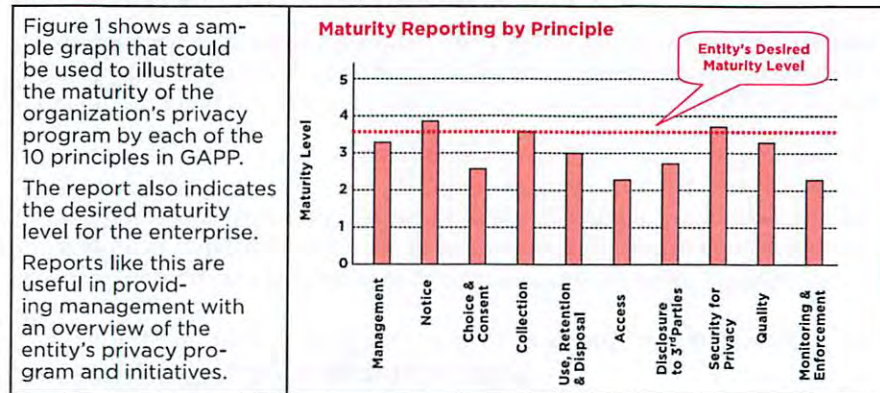


Figure 2 - Maturity Report by Criteria within a Specific GAPP Principle

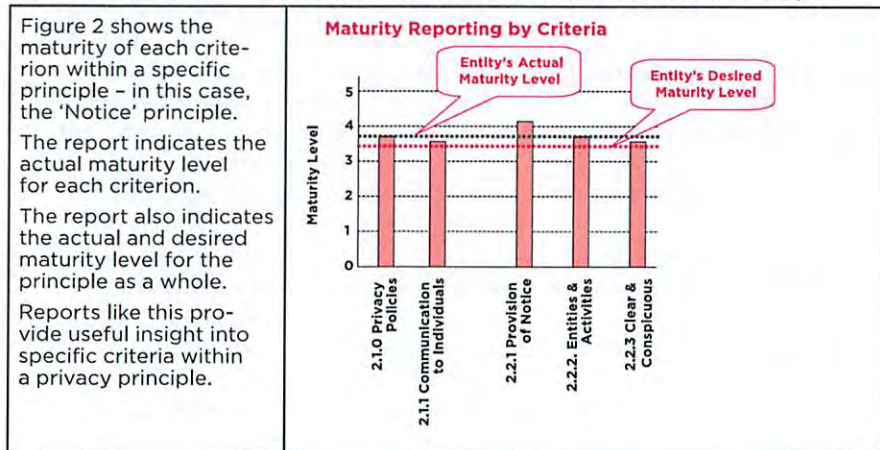
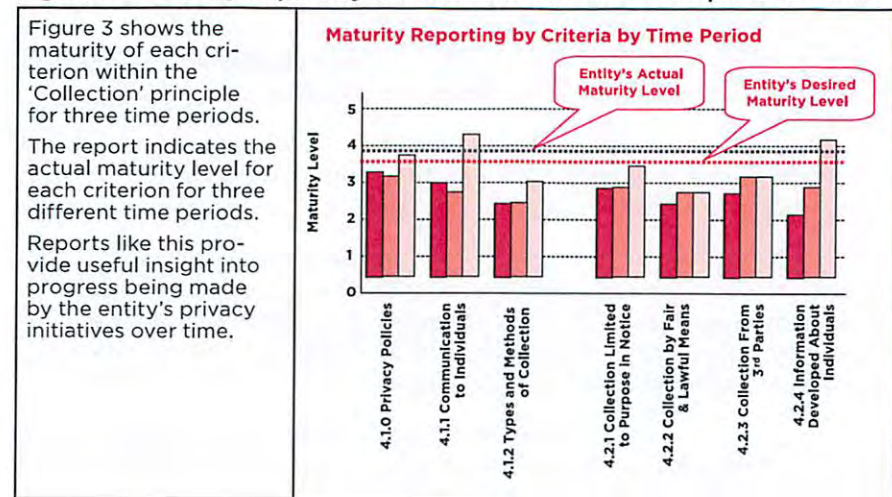


Figure 3 - Maturity Report by Criteria within a GAPP Principle Over Time



6 SUMMARY

The AICPA/CICA Privacy Maturity Model provides entities with an opportunity to assess their privacy initiatives against criteria that reflect the maturity of their privacy program and their level of compliance with Generally Accepted Privacy Principles.

The PMM can be a useful tool for management, consultants and auditors and should be considered throughout the entity's journey to develop a strong privacy program and benchmark its progress.

AICPA/CICA PRIVACY MATURITY MODEL¹

Based on Generally Accepted Privacy Principles (GAPP)²

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria)	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Privacy Policies (1.1.0)	The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.	Some aspects of privacy policies exist informally.	Privacy policies exist but may not be complete, and are not fully documented.	Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.	Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with policies and procedures concerning personal information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.
Communication to Internal Personnel (1.1.1)	Privacy policies and the consequences of non-compliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	Employees may be informed about the entity's privacy policies; however, communications are inconsistent, sporadic and undocumented.	Employees are provided guidance on the entity's privacy policies and procedures through various means; however, formal policies, where they exist, are not complete.	The entity has a process in place to communicate privacy policies and procedures to employees through initial awareness and training sessions and an ongoing communications program.	Privacy policies and the consequences of non-compliance are communicated at least annually; understanding is monitored and assessed.	Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback. Changes in privacy policies are communicated to personnel shortly after the changes are approved.

¹ This model is based on Technical Report, CMU/SEI-93TR-024 ESC-TR-93-177, "Capability Maturity Model SM for Software, Version 1.1," Copyright 1993 Carnegie Mellon University, with special permission from the Software Engineering Institute. Any material of Carnegie Mellon University and/or its Software Engineering Institute contained herein is furnished on an "as-is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement. This model has not been reviewed nor is it endorsed by Carnegie Mellon University or its Software Engineering Institute. © Capability Maturity Model, CMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

² Published by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA)

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Responsibility and Accountability for Policies (1.1.2)	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	Management is becoming aware of privacy issues but has not yet identified a key sponsor or assigned responsibility. Privacy issues are addressed reactively.	Management understands the risks, requirements (including legal, regulatory and industry) and their responsibilities with respect to privacy. There is an understanding that appropriate privacy management is important and needs to be considered. Responsibility for operation of the entity's privacy program is assigned; however, the approaches are often informal and fragmented with limited authority or resources allocated.	Defined roles and responsibilities have been developed and assigned to various individuals / groups within the entity and employees are aware of those assignments. The approach to developing privacy policies and procedures is formalized and documented.	Management monitors the assignment of roles and responsibilities to ensure they are being performed, that the appropriate information and materials are developed and that those responsible are communicating effectively. Privacy initiatives have senior management support.	The entity (such as a committee of the board of directors) regularly monitors the processes and assignments of those responsible for privacy and analyzes the progress to determine its effectiveness. Where required, changes and improvements are made in a timely and effective fashion.
Review and Approval (1.2.1)	Privacy policies and procedures, and changes thereto, are reviewed and approved by management.	Reviews are informal and not undertaken on a consistent basis.	Management undertakes periodic review of privacy policies and procedures; however, little guidance has been developed for such reviews.	Management follows a defined process that requires their review and approval of privacy policies and procedures.	The entity has supplemented management review and approval with periodic reviews by both internal and external privacy specialists.	Management's review and approval of privacy policies also include periodic assessments of the privacy program to ensure all changes are warranted, made and approved; if necessary, the approval process will be revised.
Consistency of Privacy Policies and Procedures with Laws and Regulations (1.2.2)	Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	Reviews and comparisons with applicable laws and regulations are performed inconsistently and are incomplete.	Privacy policies and procedures have been reviewed to ensure their compliance with applicable laws and regulations; however, documented guidance is not provided.	A process has been implemented that requires privacy policies to be periodically reviewed and maintained to reflect changes in privacy legislation and regulations; however, there is no proactive review of legislation.	Changes to privacy legislation and regulations are reviewed by management and changes are made to the entity's privacy policies and procedures as required. Management may subscribe to a privacy service that regularly informs them of such changes.	Management assesses the degree to which changes to legislation are reflected in their privacy policies.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Personal Information Identification and Classification (1.2.3)	The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures.	The identification of personal information is irregular, incomplete, inconsistent, and potentially out of date. Personal information is not adequately addressed in the entity's privacy and related security policies and procedures. Personal information may not be differentiated from other information.	Basic categories of personal information have been identified and covered in the entity's security and privacy policies; however, the classification may not have been extended to all personal information.	All personal information collected, used, stored and disclosed within the entity has been classified and risk rated.	All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance. Personal information records are reviewed to ensure appropriate classification.	Management maintains a record of all instances and uses of personal information. In addition, processes are in place to ensure changes to business processes and procedures and any supporting computerized systems, where personal information is involved, result in an updating of personal information records. Personal information records are reviewed to ensure appropriate classification.
Risk Assessment (1.2.4)	A risk assessment process is used to establish a risk baseline and, at least annually, to identify new or changed risks to personal information and to develop and update responses to such risks.	Privacy risks may have been identified, but such identification is not the result of any formal process. The privacy risks identified are incomplete and inconsistent. A privacy risk assessment has not likely been completed and privacy risks not formally documented.	Employees are aware of and consider various privacy risks. Risk assessments may not be conducted regularly, are not part of a more thorough risk management program and may not cover all areas.	Processes have been implemented for risk identification, risk assessment and reporting. A documented framework is used and risk appetite is established. For risk assessment, organizations may wish to use the AICPA/CICA Privacy Risk Assessment Tool.	Privacy risks are reviewed annually both internally and externally. Changes to privacy policies and procedures and the privacy program are updated as necessary.	The entity has a formal risk management program that includes privacy risks which may be customized by jurisdiction, business unit or function. The program maintains a risk log that is periodically assessed. A formal annual risk management review is undertaken to assess the effectiveness of the program and changes are made where necessary. A risk management plan has been implemented.
Consistency of Commitments with Privacy Policies and Procedures (1.2.5)	Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.	Reviews of contracts for privacy considerations are incomplete and inconsistent.	Procedures exist to review contracts and other commitments for instances where personal information may be involved; however, such reviews are informal and not consistently used.	A log of contracts exists and all contracts are reviewed for privacy considerations and concerns prior to execution.	Existing contracts are reviewed upon renewal to ensure continued compliance with the privacy policies and procedures. Changes in the entity's privacy policies will trigger a review of existing contracts for compliance.	Contracts are reviewed on a regular basis and tracked. An automated process has been set up to flag which contracts require immediate review when changes to privacy policies and procedures are implemented.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Infrastructure and Systems Management (1.2.6)	<p>The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following:</p> <ul style="list-style-type: none"> • Infrastructure • Systems • Applications • Web sites • Procedures • Products and services • Data bases and information repositories • Mobile computing and other similar electronic devices <p>The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with the entity's privacy policies and procedures.</p>	Changes to existing processes or the implementation of new business and system processes for privacy issues is not consistently assessed.	Privacy impact is considered during changes to business processes and/or supporting application systems; however, these processes are not fully documented and the procedures are informal and inconsistently applied.	The entity has implemented formal procedures to assess the privacy impact of new and significantly changed products, services, business processes and infrastructure (sometimes referred to as a privacy impact assessment). The entity uses a documented systems development and change management process for all information systems and related technology employed to collect, use, retain, disclose and destroy personal information.	Management monitors and reviews compliance with policies and procedures that require a privacy impact assessment.	Through quality reviews and other independent assessments, management is informed of the effectiveness of the process for considering privacy requirements in all new and modified processes and systems. Such information is analyzed and, where necessary, changes made.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Privacy Incident and Breach Management (1.2.7)	<p>A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following:</p> <ul style="list-style-type: none"> • Procedures for the identification, management and resolution of privacy incidents and breaches • Defined responsibilities • A process to identify incident severity and determine required actions and escalation procedures • A process for complying with breach laws and regulations, including stakeholder breach notification, if required • An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties or discipline, as appropriate • A process for periodic review (at least annually) of actual incidents to identify necessary program updates based on the following: <ul style="list-style-type: none"> — Incident patterns and root cause — Changes in the internal control environment or external requirements (regulation or legislation) • Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed 	Few procedures exist to identify and manage privacy incidents; however, they are not documented and are applied inconsistently.	Procedures have been developed on how to deal with a privacy incident; however, they are not comprehensive and/or inadequate employee training has increased the likelihood of unstructured and inconsistent responses.	A documented breach management plan has been implemented that includes: accountability, identification, risk assessment, response, containment, communications (including possible notification to affected individuals and appropriate authorities, if required or deemed necessary), remediation (including post-breach analysis of the breach response) and resumption.	A walkthrough of the breach management plan is performed periodically and updates to the program are made as needed.	The internal and external privacy environments are monitored for issues affecting breach risk and breach response, evaluated and improvements are made. Management assessments are provided after any privacy breach and analyzed; changes and improvements are made.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Supporting Resources (1.2.8)	Resources are provided by the entity to implement and support its privacy policies.	Resources are only allocated on an "as needed" basis to address privacy issues as they arise.	Privacy procedures exist; however, they have been "developed" within small units or groups without support from privacy specialists.	Individuals with responsibility and/or accountability for privacy are empowered with appropriate authority and resources. Such resources are made available throughout the entity.	Management ensures that adequately qualified privacy resources are identified and made available throughout the entity to support its various privacy initiatives.	Management annually reviews its privacy program and seeks ways to improve the program's performance, including assessing the adequacy, availability and performance of resources.
Qualifications of Internal Personnel (1.2.9)	The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received the necessary training.	The entity has not formally established qualifications for personnel who collect, use, disclose or otherwise handle personal information.	The entity has some established qualifications for personnel who collect, disclose, use or otherwise handle personal information, but are not fully documented. Employees receive some training on how to deal with personal information.	The entity defines qualifications for personnel who perform or manage the entity's collection, use and disclosure of personal information. Persons responsible for the protection and security of personal information have received appropriate training and have the necessary knowledge to manage the entity's collection, use and disclosure of personal information.	The entity has formed a nucleus of privacy-qualified individuals to provide privacy support to assist with specific issues, including training and job assistance.	The entity annually assesses the performance of their privacy program, including the performance and qualifications of their privacy-designated specialists. An analysis is performed of the results and changes or improvements made, as required.
Privacy Awareness and Training (1.2.10)	A privacy awareness program about the entity's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.	Formal privacy training is not provided to employees; however some knowledge of privacy may be obtained from other employees or anecdotal sources.	The entity has a privacy awareness program, but training is sporadic and inconsistent.	Personnel who handle personal information have received appropriate privacy awareness and training to ensure the entity meets obligations in its privacy notice and applicable laws. Training is scheduled, timely and consistent.	An enterprise-wide privacy awareness and training program exists and is monitored by management to ensure compliance with specific training requirements. The entity has determined which employees require privacy training and tracks their participation during such training.	A strong privacy culture exists. Compulsory privacy awareness and training is provided. Such training requires employees to complete assignments to validate their understanding. When privacy incidents or breaches occur, remedial training as well as changes to the training curriculum is made in a timely fashion.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Changes in Regulatory and Business Requirements (1.2.11)	<p>For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed:</p> <ul style="list-style-type: none"> – Legal and regulatory – Contracts, including service-level agreements – Industry requirements – Business operations and processes – People, roles, and responsibilities – Technology <p>Privacy policies and procedures are updated to reflect changes in requirements.</p>	Changes in business and regulatory environments are addressed sporadically in any privacy initiatives the entity may contemplate. Any privacy-related issues or concerns that are identified only occur in an informal manner.	The entity is aware that certain changes may impact their privacy initiatives; however, the process is not fully documented.	The entity has implemented policies and procedures designed to monitor and act upon changes in the business and/or regulatory environment. The procedures are inclusive and employees receive training in their use as part of an enterprise-wide privacy program.	The entity has established a process to monitor the privacy environment and identify items that may impact its privacy program. Changes are considered in terms of the entity's legal, contracting, business, human resources and technology.	The entity has established a process to continually monitor and update any privacy obligations that may arise from changes to legislation, regulations, industry-specific requirements and business practices.
NOTICE (5 criteria)	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.					
Privacy Policies (2.1.0)	The entity's privacy policies address providing notice to individuals.	Notice policies and procedures exist informally.	Notice provisions exist in privacy policies and procedures but may not cover all aspects and are not fully documented.	Notice provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with notice provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to notice. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (2.1.1)	<p>Notice is provided to individuals regarding the following privacy policies: purpose; choice/consent; collection; use/retention/disposal; access; disclosure to third parties; security for privacy; quality; and monitoring/enforcement.</p> <p>If personal information is collected from sources other than the individual, such sources are described in the notice.</p>	Notice to individuals is not provided in a consistent manner and may not include all aspects of privacy, such as purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Notice is provided to individuals regarding some of the following privacy policies at or before the time of collection: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Notice is provided to individuals regarding all of the following privacy policies at or before collection and is documented: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Privacy policies describe the consequences, if any, of not providing the requested information and indicate that certain information may be developed about individuals, such as buying patterns, or collected from other sources.	Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
NOTICE (5 criteria) cont.	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.					
Provision of Notice (2.2.1)	Notice is provided to the individual about the entity's privacy policies and procedures (a) at or before the time personal information is collected, or as soon as practical thereafter, (b) at or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, or (c) before personal information is used for new purposes not previously identified.	Notice may not be readily accessible nor provided on a timely basis.	Notice provided to individuals is generally accessible but is not provided on a timely basis. Notice may not be provided in all cases when personal information is collected or used for new purposes.	The privacy notice is documented, readily accessible and available, provided in a timely fashion and clearly dated.	The entity tracks previous iterations of the privacy policies and individuals are informed about changes to a previously communicated privacy notice. The privacy notice is updated to reflect changes to policies and procedures.	The entity solicits input from relevant stakeholders regarding the appropriate means of providing notice and makes changes as deemed appropriate. Notice is provided using various techniques to meet the communications technologies of their constituents (e.g. social media, mobile communications, etc).
Entities and Activities Covered (2.2.2)	An objective description of the entities and activities covered by privacy policies is included in the privacy notice.	The privacy notice may not include all relevant entities and activities.	The privacy notice describes some of the particular entities, business segments, locations, and types of information covered.	The privacy notice objectively describes and encompasses all relevant entities, business segments, locations, and types of information covered.	The entity performs a periodic review to ensure the entities and activities covered by privacy policies are updated and accurate.	Management follows a formal documented process to consider and take appropriate action as necessary to update privacy policies and the privacy notice prior to any change in the entity's business structure and activities.
Clear and Conspicuous (2.2.3)	The privacy notice is conspicuous and uses clear language.	Privacy policies are informal, not documented and may be phrased differently when orally communicated.	The privacy notice may be informally provided but is not easily understood, nor is it easy to see or easily available at points of data collection. If a formal privacy notice exists, it may not be clear and conspicuous.	The privacy notice is in plain and simple language, appropriately labeled, easy to see, and not in small print. Privacy notices provided electronically are easy to access and navigate.	Similar formats are used for different and relevant subsidiaries or segments of an entity to avoid confusion and allow consumers to identify any differences. Notice formats are periodically reviewed for clarity and consistency.	Feedback about improvements to the readability and content of the privacy policies are analyzed and incorporated into future versions of the privacy notice.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
CHOICE and CONSENT (7 criteria)	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.					
Privacy Policies (3.1.0)	The entity's privacy policies address the choices to individuals and the consent to be obtained.	Choice and consent policies and procedures exist informally.	Choice and consent provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Choice and consent provisions in privacy policies and procedures cover all relevant aspects and are fully documented.	Compliance with choice and consent provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to choice and consent. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (3.1.1)	Individuals are informed about (a) the choices available to them with respect to the collection, use, and disclosure of personal information, and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.	Individuals may be informed about the choices available to them; however, communications are inconsistent, sporadic and undocumented.	The entity's privacy notice describes in a clear and concise manner some of the following: 1) choices available to the individual regarding collection, use, and disclosure of personal information, 2) the process an individual should follow to exercise these choices, 3) the ability of, and process for, an individual to change contact preferences and 4) the consequences of failing to provide personal information required.	The entity's privacy notice describes, in a clear and concise manner, all of the following: 1) choices available to the individual regarding collection, use, and disclosure of personal information, 2) the process an individual should follow to exercise these choices, 3) the ability of, and process for, an individual to change contact preferences and 4) the consequences of failing to provide personal information required.	Privacy policies and procedures are reviewed periodically to ensure the choices available to individuals are updated as necessary and the use of explicit or implicit consent is appropriate with regard to the personal information being used or disclosed.	Changes and improvements to messaging and communications techniques and technologies are made in response to periodic assessments and feedback.
Consequences of Denying or Withdrawing Consent (3.1.2)	When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.	Individuals may not be informed consistently about the consequences of refusing, denying or withdrawing.	Consequences may be identified but may not be fully documented or consistently disclosed to individuals.	Individuals are informed about the consequences of refusing to provide personal information or denying or withdrawing consent.	Processes are in place to review the stated consequences periodically to ensure completeness, accuracy and relevance.	Processes are implemented to reduce the consequences of denying consent, such as increasing the granularity of the application of such consequences.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
CHOICE and CONSENT (7 criteria) cont.	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.					
Implicit or Explicit Consent (3.2.1)	Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual's preferences expressed in his or her consent are confirmed and implemented.	Consent is neither documented nor consistently obtained at or before collection of personal information.	Consent is consistently obtained, but may not be documented or obtained in a timely fashion.	Consent is obtained before or at the time personal information is collected and preferences are implemented (such as making appropriate database changes and ensuring that programs that access the database test for the preference). Explicit consent is documented and implicit consent processes are appropriate. Processes are in place to ensure that consent is recorded by the entity and referenced prior to future use.	An individual's preferences are confirmed and any changes are documented and referenced prior to future use.	Consent processes are periodically reviewed to ensure the individual's preferences are being appropriately recorded and acted upon and, where necessary, improvements made. Automated processes are followed to test consent prior to use of personal information.
Consent for New Purposes and Uses (3.2.2)	If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified and implicit or explicit consent is obtained prior to such new use or purpose.	Individuals are not consistently notified about new proposed uses of personal information previously collected.	Individuals are consistently notified about new purposes not previously specified. A process exists to notify individuals but may not be fully documented and consent might not be obtained before new uses.	Consent is obtained and documented prior to using personal information for purposes other than those for which it was originally collected.	Processes are in place to ensure personal information is used only in accordance with the purposes for which consent has been obtained and to ensure it is not used if consent is withdrawn. Monitoring is in place to ensure personal information is not used without proper consent.	Consent processes are periodically reviewed to ensure consent for new purposes is being appropriately recorded and acted upon and where necessary, improvements made. Automated processes are followed to test consent prior to use of personal information.
Explicit Consent for Sensitive Information (3.2.3)	Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.	Explicit consent is not consistently obtained prior to collection of sensitive personal information.	Employees who collect personal information are aware that explicit consent is required when obtaining sensitive personal information; however, the process is not well defined or fully documented.	A documented formal process has been implemented requiring explicit consent be obtained directly from the individual prior to, or as soon as practically possible, after collection of sensitive personal information.	The process is reviewed and compliance monitored to ensure explicit consent is obtained prior to, or as soon as practically possible, after collection of sensitive personal information.	For procedures that collect sensitive personal information and do not obtain explicit consent, remediation plans are identified and implemented to ensure explicit consent has been obtained.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
CHOICE and CONSENT (7 criteria) cont.	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.					
Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices (3.2.4)	Consent is obtained before personal information is transferred to/from an individual's computer or similar device.	Consent is not consistently obtained before personal information is transferred to/from another computer or other similar device.	Software enables an individual to provide consent before personal information is transferred to/from another computer or other similar device.	The application is designed to consistently solicit and obtain consent before personal information is transferred to/from another computer or other similar device and does not make any such transfers if consent has not been obtained. Such consent is documented.	The process is reviewed and compliance monitored to ensure consent is obtained before any personal information is transferred to/from an individual's computer or other similar device.	Where procedures have been identified that do not obtain consent before personal information is transferred to/from an individual's computer or other similar device, remediation plans are identified and implemented.
COLLECTION (7 criteria)	The entity collects personal information only for the purposes identified in the notice.					
Privacy Policies (4.1.0)	The entity's privacy policies address the collection of personal information.	Collection policies and procedures exist informally.	Collection provisions in privacy policies and procedures exist but might not cover all aspects, and are not fully documented.	Collection provisions in privacy policies cover all relevant aspects of collection and are fully documented.	Compliance with collection provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to collection. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (4.1.1)	Individuals are informed that personal information is collected only for the purposes identified in the notice.	Individuals may be informed that personal information is collected only for purposes identified in the notice; however, communications are inconsistent, sporadic and undocumented.	Individuals are informed that personal information is collected only for the purposes identified in the notice. Such notification is generally not documented.	Individuals are informed that personal information is collected only for the purposes identified in the notice and the sources and methods used to collect this personal information are identified. Such notification is available in written format.	Privacy policies are reviewed periodically to ensure the areas related to collection are updated as necessary.	Changes and improvements to messaging and communications methods and techniques are made in response to periodic assessments and feedback.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
COLLECTION (7 criteria) cont.	The entity collects personal information only for the purposes identified in the notice.					
Types of Personal Information Collected and Methods of Collection (4.1.2)	The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.	Individuals may be informed about the types of personal information collected and the methods of collection; however, communications are informal, may not be complete and may not fully describe the methods of collection.	The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are neither fully documented nor fully described in the privacy notice.	The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are fully documented and fully described in the privacy notice. The notice also discloses whether information is developed or acquired about individuals, such as buying patterns. The notice also describes the consequences if the cookie is refused.	Management monitors business processes to identify new types of personal information collected and new methods of collection to ensure they are described in the privacy notice.	The privacy notice is reviewed regularly and updated in a timely fashion to describe all the types of personal information being collected and the methods used to collect them.
Collection Limited to Identified Purpose (4.2.1)	The collection of personal information is limited to that necessary for the purposes identified in the notice.	Informal and undocumented procedures are relied upon to ensure collection is limited to that necessary for the purposes identified in the privacy notice.	Policies and procedures, may not: <ul style="list-style-type: none"> • be fully documented; • distinguish the personal information essential for the purposes identified in the notice; • differentiate personal information from optional information. 	Policies and procedures that have been implemented are fully documented to clearly distinguish the personal information essential for the purposes identified in the notice and differentiate it from optional information. Collection of personal information is limited to information necessary for the purposes identified in the privacy notice.	Policies and procedures are in place to periodically review the entity's needs for personal information.	Policies, procedures and business processes are updated due to changes in the entity's needs for personal information. Corrective action is undertaken when information not necessary for the purposes identified is collected.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
COLLECTION (7 criteria) cont.	The entity collects personal information only for the purposes identified in the notice.					
Collection by Fair and Lawful Means (4.2.2)	Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.	Informal procedures exist limiting the collection of personal information to that which is fair and lawful; however, they may be incomplete and inconsistently applied.	Management may conduct reviews of how personal information is collected, but such reviews are inconsistent and untimely. Policies and procedures related to the collection of personal information are either not fully documented or incomplete.	Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.	Methods of collecting personal information are periodically reviewed by management after implementation to confirm personal information is obtained fairly and lawfully.	Complaints to the entity are reviewed to identify where unlawful or deceptive practices exist. Such complaints are reviewed, analyzed and changes to policies and procedures to correct such practices are implemented.
Collection from Third Parties (4.2.3)	Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.	Limited guidance and direction exist to assist in the review of third-party practices regarding collection of personal information.	Reviews of third-party practices are performed but such procedures are not fully documented.	The entity consistently reviews privacy policies, collection methods, and types of consents of third parties before accepting personal information from third-party data sources. Clauses are included in agreements that require third-parties to collect information fairly and lawfully and in accordance with the entity's privacy policies.	Once agreements have been implemented, the entity conducts a periodic review of third-party collection of personal information. Corrective actions are discussed with third parties.	Lessons learned from contracting and contract management processes are analyzed and, where appropriate, improvements are made to existing and future contracts involving collection of personal information involving third parties.
Information Developed About Individuals (4.2.4)	Individuals are informed if the entity develops or acquires additional information about them for its use.	Policies and procedures informing individuals that additional information about them is being collected or used are informal, inconsistent and incomplete.	Policies and procedures exist to inform individuals when the entity develops or acquires additional personal information about them for its use; however, procedures are not fully documented or consistently applied.	The entity's privacy notice indicates that, if applicable, it may develop and/or acquire information about individuals by using third-party sources, browsing, e-mail content, credit and purchasing history. Additional consent is obtained where necessary.	The entity monitors information collection processes, including the collection of additional information, to ensure appropriate notification and consent requirements are complied with. Where necessary, changes are implemented.	The entity's privacy notice provides transparency in the collection, use and disclosure of personal information. Individuals are given multiple opportunities to learn how personal information is developed or acquired.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
USE, RETENTION AND DISPOSAL (5 criteria)	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.					
Privacy Policies (5.1.0)	The entity's privacy policies address the use, retention, and disposal of personal information.	Procedures for the use, retention and disposal of personal information are ad hoc, informal and likely incomplete.	Use, retention and disposal provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Use, retention and disposal provisions in privacy policies and procedures cover all relevant aspects and are fully documented.	Compliance with use, retention and disposal provisions in privacy policies and procedures is monitored.	Management monitors compliance with privacy policies and procedures relating to use, retention and disposal. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.
Communication to Individuals (5.1.1)	Individuals are informed that personal information is (a) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (b) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (c) disposed of in a manner that prevents loss, theft, misuse or unauthorized access.	Individuals may be informed about the uses, retention and disposal of their personal information; however, communications are inconsistent, sporadic and undocumented.	Individuals are informed about the use, retention and disposal of personal information, but this communication may not cover all aspects and is not fully documented. Retention periods are not uniformly communicated.	Individuals are consistently and uniformly informed about use, retention and disposal of personal information. Data retention periods are identified and communicated to individuals.	Methods are in place to update communications to individuals when changes occur to use, retention and disposal practices.	Individuals' general level of understanding of use, retention and disposal of personal information is assessed. Feedback is used to continuously improve communication methods.
Use of Personal Information (5.2.1)	Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	The use of personal information may be inconsistent with the purposes identified in the notice. Consent is not always obtained consistently.	Policies and procedures regarding the use of information have been adopted; however, they are not documented and may not be consistently applied.	Use of personal information is consistent with the purposes identified in the privacy notice. Consent for these uses is consistently obtained. Uses of personal information throughout the entity are in accordance with the individual's preferences and consent.	Uses of personal information are monitored and periodically reviewed for appropriateness. Management ensures that any discrepancies are corrected on a timely basis.	The uses of personal information are monitored and periodically assessed for appropriateness; verifications of consent and usage are conducted through the use of automation. Any discrepancies are remediated in a timely fashion. Changes to laws and regulations are monitored and the entity's policies and procedures are amended as required.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
USE, RETENTION AND DISPOSAL (5 criteria) cont.	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.					
Retention of Personal Information (5.2.2)	Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.	The retention of personal information is irregular and inconsistent.	Policies and procedures for identifying retention periods of personal information have been adopted, but may not be fully documented or cover all relevant aspects.	The entity has documented its retention policies and procedures and consistently retains personal information in accordance with such policies and practices.	Retention practices are periodically reviewed for compliance with policies and changes implemented when necessary.	The retention of personal information is monitored and periodically assessed for appropriateness, and verifications of retention are conducted. Such processes are automated to the extent possible. Any discrepancies found are remediated in a timely fashion.
Disposal, Destruction and Redaction of Personal Information (5.2.3)	Personal information no longer retained is anonymized, disposed of or destroyed in a manner that prevents loss, theft, misuse or unauthorized access.	The disposal, destruction and redaction of personal information is irregular, inconsistent and incomplete.	Policies and procedures for identifying appropriate and current processes and techniques for the appropriate disposal, destruction and redaction of personal information have been adopted but are not fully documented or complete.	The entity has documented its policies and procedures regarding the disposal, destruction and redaction of personal information, implemented such practices and ensures that these practices are consistent with the privacy notice.	The disposal, destruction, and redaction of personal information are consistently documented and periodically reviewed for compliance with policies and appropriateness.	The disposal, destruction, and redaction of personal information are monitored and periodically assessed for appropriateness, and verification of the disposal, destruction and redaction conducted. Such processes are automated to the extent possible. Any discrepancies found are remediated in a timely fashion.
ACCESS (8 criteria)	The entity provides individuals with access to their personal information for review and update.					
Privacy Policies (6.1.0)	The entity's privacy policies address providing individuals with access to their personal information.	Informal access policies and procedures exist.	Access provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Access provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Compliance with access provisions in privacy policies and procedures is monitored.	Management monitors compliance with privacy policies and procedures relating to access. Issues of non-compliance are identified and remedial action taken to ensure compliance.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
ACCESS (8 criteria) cont.	The entity provides individuals with access to their personal information for review and update.					
Communication to Individuals (6.1.1)	Individuals are informed about how they may obtain access to their personal information to review, update and correct that information.	Individuals may be informed about how they may obtain access to their personal information; however, communications are inconsistent, sporadic and undocumented.	Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly communicated.	Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly communicated.	Processes are in place to update communications to individuals when changes occur to access policies, procedures and practices.	The entity ensures that individuals are informed about their personal information access rights, including update and correction options, through channels such as direct communication programs, notification on statements and other mailings and training and awareness programs for staff. Management monitors and assesses the effects of its various initiatives and seeks to continuously improve methods of communication and understanding.
Access by Individuals to their Personal Information (6.2.1)	Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.	The entity has informal procedures granting individuals access to their information; however, such procedures are not be documented and may not be consistently applied.	Some procedures are in place to allow individuals to access their personal information, but they may not cover all aspects and may not be fully documented.	Procedures to search for an individual's personal information and to grant individuals access to their information have been documented, implemented and cover all relevant aspects. Employees have been trained in how to respond to these requests, including recording such requests.	Procedures are in place to ensure individuals receive timely communication of what information the entity maintains about them and how they can obtain access. The entity monitors information and access requests to ensure appropriate access to such personal information is provided. The entity identifies and implements measures to improve the efficiency of its searches for an individual's personal information.	The entity reviews the processes used to handle access requests to determine where improvements may be made and implements such improvements. Access to personal information is automated and self-service when possible and appropriate.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
ACCESS (8 criteria) cont.	The entity provides individuals with access to their personal information for review and update.					
Confirmation of an Individual's Identity (6.2.2)	The identity of individuals who request access to their personal information is authenticated before they are given access to that information.	Procedures to authenticate individuals requesting access to their information are informal, not documented and may not be consistently applied.	Procedures are in place to confirm the identity of individuals requesting access to their personal information before they are granted access, but do not cover all aspects and may not be documented. Level of authentication required may not be appropriate to the personal information being accessed.	Confirmation/authentication methods have been implemented to uniformly and consistently confirm the identity of individuals requesting access to their personal information, including the training of employees.	Procedures are in place to track and monitor the confirmation/authentication of individuals before they are granted access to personal information, and to review the validity of granting access to such personal information.	The successful confirmation/authentication of individuals before they are granted access to personal information is monitored and periodically assessed for type 1 (where errors are not caught) and type 2 (where an error has been incorrectly identified) errors. Remediation plans to lower the error rates are formulated and implemented.
Understandable Personal Information, Time Frame, and Cost (6.2.3)	Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.	The entity has some informal procedures designed to provide information to individuals in an understandable form. Timeframes and costs charged may be inconsistent and unreasonable.	Procedures are in place requiring that personal information be provided to the individual in an understandable form, in a reasonable timeframe and at a reasonable cost, but may not be fully documented or cover all aspects.	Procedures have been implemented that consistently and uniformly provide personal information to the individual in an understandable form, in a reasonable timeframe and at a reasonable cost.	Procedures are in place to track and monitor the response time in providing personal information, the associated costs incurred by the entity and any charges to the individual making the request. Periodic assessments of the understandability of the format for information provided to individuals are conducted.	Reports of response times in providing personal information are monitored and assessed. The associated costs incurred by the entity and any charges to the individual making the request are periodically assessed. Periodic assessments of the understandability of the format for information provided to individuals are conducted. Remediation plans are made and implemented for unacceptable response time, excessive or inconsistent charges and difficult-to-read personal information report formats. Conversion of personal information to an understandable form is automated where possible and appropriate.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
ACCESS (8 criteria) cont.	The entity provides individuals with access to their personal information for review and update.					
Denial of Access (6.2.4)	Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.	Informal procedures are used to inform individuals, of the reason a request for access to their personal information was denied; however they are incomplete and inconsistently applied.	Procedures are in place to inform individuals of the reason a request for access to their personal information was denied, but they may not be documented or cover all aspects. Notification may not be in writing or include the entity's legal rights to deny such access and the individual's right to challenge denials.	Consistently applied and uniform procedures have been implemented to inform individuals in writing of the reason a request for access to their personal information was denied. The entity's legal rights to deny such access have been identified as well as the individual's right to challenge denials.	Procedures are in place to review the response time to individuals whose access request has been denied, reasons for such denials, as well as any communications regarding challenges.	Reports of denial reasons, response times and challenge communications are monitored and assessed. Remediation plans are identified and implemented for unacceptable response time and inappropriate denials of access. The denial process is automated and includes electronic responses where possible and appropriate.
Updating or Correcting Personal Information (6.2.5)	Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.	Informal and undocumented procedures exist that provide individuals with information on how to update or correct personal information held by the entity; however, they are incomplete and inconsistently applied.	Some procedures are in place for individuals to update or correct personal information held by the entity, but they are not complete and may not be fully documented. A process exists to review and confirm the validity of such requests and inform third parties of changes made; however, not all of the processes are documented.	Documented policies with supporting procedures have been implemented to consistently and uniformly inform individuals of how to update or correct personal information held by the entity. Procedures have been implemented to consistently and uniformly provide updated information to third parties that previously received the individual's personal information.	Procedures are in place to track data update and correction requests and to validate the accuracy and completeness of such data. Documentation or justification is kept for not providing information updates to relevant third parties.	Reports of updates and correction requests and response time to update records are monitored and assessed. Documentation or justification for not providing information updates to relevant third parties is monitored and assessed to determine whether the economically feasible requirement was met. Updating is automated and self-service where possible and appropriate. Distribution of updated information to third parties is also automated where possible and appropriate.

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
ACCESS (8 criteria) cont.	The entity provides individuals with access to their personal information for review and update.					
Statement of Disagreement (6.2.6)	Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.	Procedures used to inform individuals of the reason a request for correction of personal information was denied, and how they may appeal are inconsistent and undocumented.	Procedures are in place to inform individuals about the reason a request for correction of personal information was denied, and how they may appeal, but they are not complete or documented.	Documented policies and procedures that cover relevant aspects have been implemented to inform individuals in writing about the reason a request for correction of personal information was denied, and how they may appeal.	Procedures are in place to track and review the reasons a request for correction of personal information was denied.	Cases that involve disagreements over the accuracy and completeness of personal information are reviewed and remediation plans are identified and implemented as appropriate. The process to complete a Statement of Disagreement is automated where possible and appropriate.
DISCLOSURE TO THIRD PARTIES (7 criteria)	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.					
Privacy Policies (7.1.0)	The entity's privacy policies address the disclosure of personal information to third parties.	Informal disclosure policies and procedures exist but may not be consistently applied.	Disclosure provisions in privacy policies exist but may not cover all aspects, and are not fully documented.	Disclosure provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with disclosure provisions in privacy policies is monitored.	Management monitors compliance with privacy policies and procedures relating to disclosure to third parties. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (7.1.1)	Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise.	Individuals may be informed that personal information is disclosed to third parties only for the purposes identified in the notice; however, communications are inconsistent, sporadic and undocumented.	Procedures are in place to inform individuals that personal information is disclosed to third parties; however, limited documentation exists and the procedures may not be performed consistently or in accordance with relevant laws and regulations.	Documented procedures that cover all relevant aspects, and in accordance with relevant laws and regulations are in place to inform individuals that personal information is disclosed to third parties, but only for the purposes identified in the privacy notice and for which the individual has provided consent. Third parties or classes of third parties to whom personal information is disclosed are identified.	Procedures exist to review new or changed business processes, third parties or regulatory bodies requiring compliance to ensure appropriate communications to individuals are provided and consent obtained where necessary.	Issues identified or communicated to the entity with respect to the disclosure of personal information to third parties are monitored and, where necessary, changes and improvements made to the policies and procedures to better inform individuals.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
DISCLOSURE TO THIRD PARTIES (7 criteria) cont.	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.					
Communication to Third Parties (7.1.2)	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.	Procedures to communicate to third parties their responsibilities with respect to personal information provided to them are informal, inconsistent and incomplete.	Procedures are in place to communicate to third parties the entity's privacy policies or other specific instructions or requirements for handling personal information, but they are inconsistently applied and not fully documented.	Documented policies and procedures exist and are consistently and uniformly applied to communicate to third parties the privacy policies or other specific instructions or requirements for handling personal information. Written agreements with third parties are in place confirming their adherence to the entity's privacy policies and procedures.	A review is periodically performed to ensure third parties have received the entity's privacy policies, instructions and other requirements relating to personal information that has been disclosed. Acknowledgement of the receipt of the above is monitored.	Contracts and other agreements involving personal information provided to third parties are reviewed to ensure the appropriate information has been communicated and agreement has been obtained. Remediation plans are developed and implemented where required.
Disclosure of Personal Information (7.2.1)	Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise.	Procedures regarding the disclosure of personal information to third parties are informal, incomplete and applied inconsistently.	Procedures are in place to ensure disclosure of personal information to third parties is only for the purposes described in the privacy notice and for which the individual has provided consent, unless laws or regulations allow otherwise; however, such procedures may not be fully documented or consistently and uniformly evaluated.	Documented procedures covering all relevant aspects have been implemented to ensure disclosure of personal information to third parties is only for the purposes described in the privacy notice and for which the individual has provided consent, unless laws or regulations allow otherwise. They are uniformly and consistently applied.	Procedures are in place to test and review whether disclosure to third parties is in compliance with the entity's privacy policies.	Reports of personal information provided to third parties are maintained and such reports are reviewed to ensure only information that has consent has been provided to third parties. Remediation plans are developed and implemented where inappropriate disclosure has occurred or where third parties are not in compliance with their commitments. Disclosure to third parties may be automated.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
DISCLOSURE TO THIRD PARTIES (7 criteria) cont. Protection of Personal Information (7.2.2)	<p>The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.</p> <p>Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.</p>	<p>Procedures used to ensure third-party agreements are in place to protect personal information prior to disclosing to third parties are informal, incomplete and inconsistently applied. The entity does not have procedures to evaluate the effectiveness of third-party controls to protect personal information.</p>	<p>Procedures are in place to ensure personal information is disclosed only to third parties that have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements, but are not consistently and uniformly applied or fully documented. Some procedures are in place to determine whether third parties have reasonable controls; however, they are not consistently and uniformly assessed.</p>	<p>Documented policies and procedures covering all relevant aspects have been implemented to ensure personal information is disclosed only to third parties that have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures to evaluate whether third parties have effective controls to meet the terms of the agreement, instructions or requirements.</p>	<p>An assessment of third party procedures is periodically performed to ensure such procedures continue to meet the entity's requirements. Such assessments may be performed by the entity or an independent qualified third party.</p>	<p>Changes in a third-party environment are monitored to ensure the third party can continue to meet its obligations with respect to personal information disclosed to them. Remediation plans are developed and implemented where necessary. The entity evaluates compliance using a number of approaches to obtain an increasing level of assurance depending on its risk assessment.</p>
New Purposes and Uses (7.2.3)	<p>Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.</p>	<p>Procedures to ensure the proper disclosure of personal information to third parties for new purposes or uses are informal, inconsistent and incomplete.</p>	<p>Procedures exist to ensure the proper disclosure of personal information to third parties for new purposes; however, they may not be consistently and uniformly applied and not fully documented.</p>	<p>Documented procedures covering all relevant aspects have been implemented to ensure the proper disclosure of personal information to third parties for new purposes. Such procedures are uniformly and consistently applied. Consent from individuals prior to disclosure is documented. Existing agreements with third parties are reviewed and updated to reflect the new purposes and uses.</p>	<p>Monitoring procedures are in place to ensure proper disclosure of personal information to third parties for new purposes. The entity monitors to ensure the newly disclosed information is only being used for the new purposes or as specified.</p>	<p>Reports of disclosure of personal information to third parties for new purposes and uses, as well as the associated consent by the individual, where applicable, are monitored and assessed, to ensure appropriate consent has been obtained and documented. Collection of consent for new purposes and uses is automated where possible and appropriate.</p>

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
DISCLOSURE TO THIRD PARTIES (7 criteria) cont.	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.					
Misuse of Personal Information by a Third Party (7.2.4)	The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	Procedures to determine and address misuse of personal information by a third party are informal, incomplete and inconsistently applied.	Procedures are in place to require remedial action in response to misuse of personal information by a third party, but they are not consistently and uniformly applied or fully documented.	Documented policies and procedures covering all relevant aspects are in place to take remedial action in response to misuse of personal information by a third party. Such procedures are consistently and uniformly applied.	Monitoring procedures are in place to track the response to misuse of personal information by a third party from initial discovery through to remedial action.	Exception reports are used to record inappropriate or unacceptable activities by third parties and to monitor the status of remedial activities. Remediation plans are developed and procedures implemented to address unacceptable or inappropriate use.
SECURITY FOR PRIVACY (9 criteria)	The entity protects personal information against unauthorized access (both physical and logical).					
Privacy Policies (8.1.0)	The entity's privacy policies (including any relevant security policies) address the security of personal information.	Security policies and procedures exist informally; however, they are based on ad hoc and inconsistent processes.	Security provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Security provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with security provisions in privacy policies and procedures is evaluated and monitored.	Management monitors compliance with privacy policies and procedures relating to security. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (8.1.1)	Individuals are informed that precautions are taken to protect personal information.	Individuals may be informed about security of personal information; however, communications are inconsistent, sporadic and undocumented.	Individuals are informed about security practices to protect personal information, but such disclosures may not cover all aspects and are not fully documented.	Individuals are informed about the entity's security practices for the protection of personal information. Security policies, procedures and practices are documented and implemented.	The entity manages its security program through periodic reviews and security assessments. Incidents and violations of its communications policy for security are investigated.	Communications explain to individuals the need for security, the initiatives the entity takes to ensure that personal information is protected and informs individuals of other activities they may want to take to further protect their information.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Information Security Program (8.2.1)	<p>A security program has been developed, documented, approved, and implemented that includes administrative, technical and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction. The security program should address, but not be limited to, the following areas³ insofar as they relate to the security of personal information:</p> <ul style="list-style-type: none"> a. Risk assessment and treatment [1.2.4] b. Security policy [8.1.0] c. Organization of information security [sections 1, 7, and 10] d. Asset management [section 1] e. Human resources security [section 1] f. Physical and environmental security [8.2.3 and 8.2.4] g. Communications and operations management [sections 1, 7, and 10] h. Access control [sections 1, 8.2, and 10] i. Information systems acquisition, development, and maintenance [1.2.6] j. Information security incident management [1.2.7] k. Business continuity management [section 8.2] l. Compliance [sections 1 and 10] 	There have been some thoughts of a privacy-focused security program, but limited in scope and perhaps undocumented.	The entity has a security program in place that may not address all areas or be fully documented.	The entity has developed, documented and promulgated its comprehensive enterprise-wide security program. The entity has addressed specific privacy-focused security requirements.	Management monitors weaknesses, periodically reviews its security program as it applies to personal information and establishes performance benchmarks.	The entity undertakes annual reviews of its security program, including external reviews, and determines the effectiveness of its procedures. The results of such reviews are used to update and improve the security program.

³ These areas are drawn from ISO/IEC 27002:2005, Information technology—Security techniques—Code of practice for information security management. Permission is granted by the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). Copies of ISO/IEC 27002 can be purchased from ANSI in the United States at <http://webstore.ansi.org/> and in Canada from the Standards Council of Canada at www.standardsstore.ca/eSpecs/index.jsp. It is not necessary to meet all of the criteria of ISO/IEC 27002:2005 to satisfy Generally Accepted Privacy Principles' criterion 8.2.1. The references associated with each area indicate the most relevant Generally Accepted Privacy Principles' criteria for this purpose.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Logical Access Controls (8.2.2)	<p>Logical access to personal information is restricted by procedures that address the following matters:</p> <ul style="list-style-type: none"> a. Authorizing and registering internal personnel and individuals b. Identifying and authenticating internal personnel and individuals c. Making changes and updating access profiles d. Granting privileges and permissions for access to IT infrastructure components and personal information e. Preventing individuals from accessing anything other than their own personal or sensitive information f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities g. Distributing output only to authorized internal personnel h. Restricting logical access to offline storage, backup data, systems and media i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) j. Preventing the introduction of viruses, malicious code, and unauthorized software 	<p>Controls over access and privileges to files and databases containing personal information are informal, inconsistent and incomplete.</p>	<p>The entity has basic security procedures; however, they do not include specific requirements governing logical access to personal information and may not provide an appropriate level of access or control over personal information.</p>	<p>The entity has documented and implemented security policies and procedures that sufficiently control access to personal information.</p> <p>Access to personal information is restricted to employees with a need for such access.</p>	<p>Management monitors logical access controls, including access attempts and violation reports for files, databases and resources containing personal information to identify areas where additional security needs improvement.</p> <p>Irregular access of authorized personnel is also monitored.</p>	<p>Access and violation attempts are assessed to determine root causes and potential exposures and remedial action plans are developed and implemented to increase the level of protection of personal information. Logical access controls are continually assessed and improved.</p> <p>Irregular access of authorized personnel is monitored, assessed and investigated where necessary.</p>

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Physical Access Controls (8.2.3)	Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).	Controls over physical access to personal information are informal, incomplete and inconsistent.	The entity has basic physical security procedures; however, they do not include specific requirements governing physical access to personal information maintained or stored in various media. Accordingly, inconsistent approaches are taken throughout the entity with respect to physically securing personal information.	The entity has implemented formal physical security policies and procedures that form the basis of specific privacy-related security procedures for physical access to personal information. Physical access to personal information is restricted to employees with a need for such access.	Management monitors physical access controls. Personal information is physically stored in secure locations. Access to such locations is restricted and monitored. Unauthorized access is investigated and appropriate action taken.	Where physical access or attempted violation of personal information has occurred, the events are analyzed and remedial action including changes to policies and procedures is adopted. This may include implementing increased use of technology, as necessary. Physical access controls are continually assessed and improved.
Environmental Safeguards (8.2.4)	Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.	Some policies and procedures exist to ensure adequate safeguards over personal information in the event of disasters or other environmental hazards; however, they are incomplete and inconsistently applied. The entity may lack a business continuity plan that would require an assessment of threats and vulnerabilities and appropriate protection of personal information.	The entity has a business continuity plan addressing certain aspects of the business. Such a plan may not specifically address personal information. Accordingly, personal information may not be appropriately protected. Business continuity plans are not well documented and have not been tested.	The entity has implemented a formal business-continuity and disaster-recovery plan that address all aspects of the business and identified critical and essential resources, including personal information in all forms and media, and provides for specifics thereof. Protection includes protection against accidental, unauthorized or inappropriate access or disclosure of personal information. The plan has been tested.	Management monitors threats and vulnerabilities as part of a business risk management program and, where appropriate, includes personal information as a specific category.	Management risk and vulnerability assessments with respect to personal information result in improvements to the protection of such information.
Transmitted Personal Information (8.2.5)	Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other non-secure networks, and wireless networks is protected by deploying industry-standard encryption technology for transferring and receiving personal information.	The protection of personal information when being transmitted or sent to another party is informal, incomplete and inconsistently applied. Security restrictions may not be applied when using different types of media to transmit personal information.	Policies and procedures exist for the protection of information during transmittal but are not fully documented; however, they may not specifically address personal information or types of media.	Documented procedures that cover all relevant aspects have been implemented and are working effectively to protect personal information when transmitted.	The entity's policies and procedures for the transmission of personal information are monitored to ensure that they meet minimum industry security standards and the entity is in compliance with such standards and their own policies and procedures. Issues of non-compliance are dealt with.	Management reviews advances in security technology and techniques and updates their security policies and procedures and supporting technologies to afford the entity the most effective protection of personal information while it is being transmitted, regardless of the media used.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.						
Personal Information on Portable Media (8.2.6)	Personal information stored on portable media or devices is protected from unauthorized access.	Controls over portable devices that contain personal information are informal, incomplete and inconsistent.	Procedures are in place to protect personal information on portable devices; however, they are not fully documented. Employees are aware of the additional risks and vulnerabilities associated with the use of portable and removable devices. Awareness of requirements to protect personal information are known and certain procedures exist to preclude or restrict the use of portable and removal devices to record, transfer and archive personal information.	The entity has implemented documented policies and procedures, supported by technology, that cover all relevant aspects and restrict the use of portable or removable devices to store personal information. The entity authorizes the devices and requires mandatory encryption.	Prior to issuance of portable or removable devices, employees are required to read and acknowledge their responsibilities for such devices and recognize the consequences of violations of security policies and procedures. Where portable devices are used, only authorized and registered devices such as portable flash drives that require encryption are permitted. Use of unregistered and unencrypted portable devices is not allowed in the entity's computing environment.	Management monitors new technologies to enhance the security of personal information stored on portable devices. They ensure the use of new technologies meets security requirements for the protection of personal information, monitor adoption and implementation of such technologies and, where such monitoring identifies deficiencies or exposures, implement remedial action.
Testing Security Safeguards (8.2.7)	Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.	Tests of security safeguards for personal information are undocumented, incomplete and inconsistent.	Periodic tests of security safeguards are performed by the IT function; however, their scope varies.	Periodic and appropriate tests of security safeguards for personal information are performed in all significant areas of the business. Test work is completed by qualified personnel such as Certified Public Accountants, Chartered Accountants, Certified Information System Auditors, or internal auditors. Test results are documented and shared with appropriate stakeholders. Tests are performed at least annually.	Management monitors the testing process, ensures tests are conducted as required by policy, and takes remedial action for deficiencies identified.	Test results are analyzed, through a defined root-cause analysis, and remedial measures documented and implemented to improve the entity's security program.

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
QUALITY (4 criteria)	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.					
Privacy Policies (9.1.0)	The entity's privacy policies address the quality of personal information.	Quality control policies and procedures exist informally.	Quality provisions in privacy policies and procedures exist, but may not cover all aspects and are not fully documented.	Quality provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with quality provisions in privacy policies and procedures is monitored and the results are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to quality. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (9.1.1)	Individuals are informed that they are responsible for providing the entity with accurate and complete personal information and for contacting the entity if correction of such information is required.	Individuals may be informed about their responsibility to provide accurate and complete personal information; however, communications are inconsistent, sporadic and undocumented.	Individuals are informed of their responsibility to provide accurate information; however, communications may not cover all aspects and may not be fully documented.	Individuals are informed of their responsibility for providing accurate and complete personal information and for contacting the entity if corrections are necessary. Such communications cover all relevant aspects and are documented.	Communications are monitored to ensure individuals are adequately informed of their responsibilities and the remedies available to them should they have complaints or issues.	Communications are monitored and analyzed to ensure the messaging is appropriate and meeting the needs of individuals and changes are being made where required.
Accuracy and Completeness of Personal Information (9.2.1)	Personal information is accurate and complete for the purposes for which it is to be used.	Procedures exist to ensure the completeness and accuracy of information provided to the entity; however, they are informal, incomplete and inconsistently applied.	Procedures are in place to ensure the accuracy and completeness of personal information; however, they are not fully documented and may not cover all aspects.	Documented policies, procedures and processes that cover all relevant aspects have been implemented to ensure the accuracy of personal information. Individuals are provided with information on how to correct data the entity maintains about them.	Processes are designed and managed to ensure the integrity of personal information is maintained. Benchmarks have been established and compliance measured. Methods are used to verify the accuracy and completeness of personal information obtained, whether from individuals directly or from third parties.	Processes are in place to monitor and measure the accuracy of personal information. Results are analyzed and modifications and improvements made.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
QUALITY (4 criteria) cont.	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.					
Relevance of Personal Information (9.2.2)	Personal information is relevant to the purposes for which it is to be used.	Some procedures are in place to ensure the personal information being collected is relevant to the defined purpose, but they are incomplete, informal and inconsistently applied.	Procedures are in place to ensure that personal information is relevant to the purposes for which it is to be used, but these procedures are not fully documented nor cover all aspects.	Documented policies and procedures that cover all relevant aspects, supported by effective processes, have been implemented to ensure that only personal information relevant to the stated purposes is used and to minimize the possibility that inappropriate information is used to make business decisions about the individual.	Processes are designed and reviewed to ensure the relevance of the personal information collected, used and disclosed.	Processes are in place to monitor the relevance of personal information collected, used and disclosed. Results are analyzed and modifications and improvements made as necessary.
MONITORING and ENFORCEMENT (7 criteria)	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
Privacy Policies (10.1.0)	The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.	Monitoring and enforcement of privacy policies and procedures are informal and ad hoc. Guidance on conducting such reviews is not documented.	Monitoring and enforcement provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Monitoring and enforcement provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with monitoring and enforcement provisions in privacy policies is monitored and results are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to monitoring and enforcement. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (10.1.1)	Individuals are informed about how to contact the entity with inquiries, complaints and disputes.	Individuals may be informed about how to contact the entity with inquiries, complaints and disputes; however, communications are inconsistent, sporadic and undocumented.	Procedures are in place to inform individuals about how to contact the entity with inquiries, complaints, and disputes but may not cover all aspects and are not fully documented.	Individuals are informed about how to contact the entity with inquiries, complaints and disputes and to whom the individual can direct complaints. Policies and procedures are documented and implemented.	Communications are monitored to ensure that individuals are adequately informed about how to contact the entity with inquiries, complaints and disputes.	Communications are monitored and analyzed to ensure the messaging is appropriate and meeting the needs of individuals and changes are being made where required. Remedial action is taken when required.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MONITORING and ENFORCEMENT (7 criteria) cont.	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
Inquiry, Complaint and Dispute Process (10.2.1)	A process is in place to address inquiries, complaints and disputes.	An informal process exists to address inquiries, complaints and disputes; however, it is incomplete and inconsistently applied.	Processes to address inquiries, complaints and disputes exist, but are not fully documented and do not cover all aspects.	Documented policies and procedures covering all relevant aspects have been implemented to deal with inquiries, complaints and disputes.	Inquiries, complaints and disputes are recorded, responsibilities assigned and addressed through a managed process. Recourse and a formal escalation process are in place to review and approve any recourse offered to individuals.	Management monitors and analyzes the process to address inquiries, complaints and disputes and makes changes to the process, where appropriate.
Dispute Resolution and Recourse (10.2.2)	Each complaint is addressed, and the resolution is documented and communicated to the individual.	Complaints are handled informally and inconsistently. Adequate documentation is not available.	Processes are in place to address complaints, but they are not fully documented and may not cover all aspects.	Documented policies and procedures covering all relevant aspects have been implemented to handle privacy complaints. Resolution of the complaints is documented.	Privacy complaints are reviewed to ensure they are addressed within a specific timeframe in a satisfactory manner; satisfaction is monitored and managed. Unresolved complaints are escalated for review by management.	Privacy complaints are monitored and analyzed and the results used to redesign and improve the privacy complaint process.
Compliance Review (10.2.3)	Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements and other contracts is reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	Review of compliance with privacy policies and procedures, laws, regulations and contracts is informal, inconsistently and incomplete.	Policies and procedures to monitor compliance with privacy policies and procedures, legislative and regulatory requirements and contracts are in place, but are not fully documented and may not cover all aspects.	Documented policies and procedures that cover all relevant aspects have been implemented that require management to review compliance with the entity's privacy policies and procedures, laws, regulations, and other requirements.	Management monitors activities to ensure the entity's privacy program remains in compliance with laws, regulations and other requirements.	Management analyzes and monitors results of compliance reviews of the entity's privacy program and proactively initiates remediation efforts to ensure ongoing and sustainable compliance.
Instances of Noncompliance (10.2.4)	Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.	Processes to handle instances of non-compliance exist, but are incomplete, informal and inconsistently applied.	Policies and procedures are in place to document non-compliance with privacy policies and procedures, but are not fully documented or do not cover all relevant aspects. Corrective and disciplinary measures may not always be documented.	Documented policies and procedures covering all relevant aspects have been implemented to handle instances of non-compliance with privacy policies and procedures. Corrective and disciplinary measures of non-compliance are fully documented.	Management monitors noncompliance with privacy policies and procedures and takes appropriate corrective and disciplinary action in a timely fashion.	Non-compliance results in disciplinary action and remedial training to correct individual behavior. In addition policies and procedures are improved to assist in full understanding and compliance.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MONITORING and ENFORCEMENT (7 criteria) cont.	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
Ongoing Monitoring (10.2.5)	Ongoing procedures are performed for monitoring the effectiveness of controls over personal information based on a risk assessment and for taking timely corrective actions where necessary.	Ongoing monitoring of privacy controls over personal information is informal, incomplete and inconsistently applied.	Monitoring of privacy controls is not fully documented and does not cover all aspects.	The entity has implemented documented policies and procedures covering all relevant aspects to monitor its privacy controls. Selection of controls to be monitored and frequency with which they are monitored are based on a risk assessment.	Monitoring of controls over personal information is performed in accordance with the entity's monitoring guidelines and results analyzed and provided to management.	Monitoring is performed and the analyzed results are used to improve the entity's privacy program. The entity monitors external sources to obtain information about their privacy "performance" and initiates changes as required.



Assessment of “Financial Assurance Securities” on SharePoint

Internal Audit Bureau – Audit Report

**Audit Report
Information Technology Audit**

**Lands
“Assessment of Financial Assurance
Securities” on SharePoint**

July 2016

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.



CONFIDENTIAL

July 25, 2016

File: 7820-31-24-151-100

MR. WILLARD HAGEN
DEPUTY MINISTER
DEPARTMENT OF LANDS

Audit Report: Assessment of “Financial Assurance Securities” on SharePoint
Audit Period: As at April 30, 2015

A. SCOPE AND OBJECTIVES

The Audit Committee approved the Department of Lands (Lands) request for an audit of the processes surrounding SharePoint used to track the “Financial Assurance Securities” (Securities). The audit objectives were to assess:

- the adequacy of policies, procedures and guidelines governing the handling of Securities recorded in SharePoint
- internal controls over the SharePoint information for relevancy, reliability, accuracy, completeness, and timeliness
- level of consistency in following the established processes
- the safeguarding of the SharePoint information and the physical Securities held
- the effectiveness and efficiency of processing Securities and financial information.

The audit did not review the process used for calculating the required value of Security or for determining acceptable forms of Security. In addition, Securities under the *Petroleum Resources Act* and the Office of the Regulator of Oil and Gas Operations were not reviewed.

The audit was conducted in conformance with the *Standards for the Professional Practice of Internal Auditing*.

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.

B. BACKGROUND

Until recently, the Federal Government had jurisdiction over most of the land in the NWT. An abundance of natural resources in the NWT attracted the attention of investors. Some natural resource developments like mines required extensive remediation once the projects were concluded. In time, the federal Department of Aboriginal Affairs and Northern Development Canada (AANDC) required the resource developers to provide financial security deposits as a type of insurance for future cost of reclamation. Federally appointed Land & Water Boards had oversight over different regions of the territory and determined the value of security required for projects in their region. These Securities were mainly in the form of cash/cheques and Irrevocable Letters of Credit.

The 2012 report by the federal Commissioner of the Environment and Sustainable Development in the Office of the Auditor General of Canada (OAG) on the management of Securities under AANDC recommended that a comprehensive inventory system be developed to provide *“consistent information by project and by regulatory authority of all securities required and held to ensure that the securities continue to meet the expected reclamation costs”*. The report noted that there was:

- lack of key data necessary for monitoring the adequacy of financial securities held
- insufficient information to ensure that environmental financial securities were enough to cover project risk
- no data on the reclamation costs that were meant to be covered by a security, or on its expiration date, or whether it had been returned or replaced
- inability to track securities throughout a project’s lifetime.

In April 2014, the GNWT inherited approximately \$500 million in Securities related to NWT resource development projects from AANDC as part of the devolution of land and water to the GNWT. The GNWT assigned the regulatory authority to:

- Department of Environment and Natural Resources (ENR) for water
- Department of Investment, Tourism and Industry (ITI) for sub-surface rights
- Lands for territorial surface rights to the NWT land.

Lands also assumed responsibility for Commissioner’s Lands, which were previously under Department of Municipal and Community Affairs.

In May 2014, Financial Management Board (FMB) approved the Lands submission for the creation of the Liabilities and Financial Assurance Division (LFA Division) comprised of 5 full time staff to “coordinate the management of financial securities for resource developments” (**Appendix A refers**).

An “Interim Departmental Protocol” was drafted to:

- “Create and implement an interim solution and process to address the posting, processing, holding and release of securities building off the existing SharePoint site
- Confirm interim roles and responsibilities of the Departments identified
- Ensure that there is an ongoing process and reliable integrated securities information that the Departments can rely on to inform operations, including securities and analysis, enforcement and the financial requirements of the GNWT; and
- Inform the development of an appropriate longer term approach that will serve the Departments and the GNWT more broadly”.

Since inception, the “Interim Departmental Protocol” has gone through a number of iterations.

The SharePoint developed and designed by the Department of Finance (Finance) contained a spreadsheet that was used to track transfer of Securities from AANDC. The LFA Division started using this tool to track Securities. As of April 2015, there were 59 SharePoint users in Lands, Finance, ENR and ITI tracking the following Securities:

Authorization type	Number of Security instruments	Value held
Environmental agreements	11	\$80,235,170
17(1)(c)(iii)		
Water licences	42	451,918,127
Land use permits	77	43,038,286
Total	17(1)(c)(iii)	

C. OVERVIEW

The GNWT inherited over \$500 million in Securities from AANDC without any supporting system to address the issues identified in the 2012 OAG report. The governance complexity for Securities increased in that the authority that was exclusively within AANDC was now shared by three GNWT departments: ENR, ITI and Lands.

The processing of high dollar value of Securities provided by developers to support their project required high level of internal controls. The foundation of any internal control framework starts with the governance framework. Staff require clear and coherent direction to plan, execute and monitor the process. With a well-defined governance framework, staff would have the direction to collect the relevant, reliable, accurate, complete and timely information for management to make decisions. These two foundational internal controls would then allow staff to demonstrate compliance to authorized processes, safeguard GNWT assets, and work toward continuous improvement.

We noted that the governance framework for Securities process was a work in progress at the time of audit. There were some internal controls present but inadequately documented. The 2014 *“Interim Departmental Protocol”* provided some clarity of roles. Overall, the governance framework for Securities lacked clarity on accountability, transparency and responsibility. The *“Interim Departmental Protocol”* continues to evolve and was not formalized as an authoritative framework for processing of Securities by multi-departments. The current governance framework was insufficient to address the GNWT risks involving millions of dollars in Security, dependency of process on multiple internal and external stakeholders, and complexity of business environment.

The interim measure of using a spreadsheet on SharePoint to track Securities lacked information integrity. The continuous manual process of reviewing the transactions for accuracy and completeness was not sustainable for an extended period of time. The capacity to manage spreadsheet data integrity could influence the development and management of a much more complex application for Securities tracking.

Strong governance framework and information integrity would form the foundation for the development of an internal control capacity to manage the GNWT Securities risk.

D. OBSERVATIONS AND RECOMMENDATIONS

1. Governance Framework

Observation

Incomplete governance framework did not allow for the effective monitoring of GNWT risk exposure for resource development projects.

The LFA Division was approved by FMB to “*coordinate the management of financial securities for resource developments*” (**Appendix A refers**). The coordination of Securities within the GNWT impacted five departments: ENR, Finance, ITI, Justice, and Lands.

The executive branch of the GNWT has established a number of governance committees to effectively coordinate processes impacting more than one department. These governance committees provide guidance to department staff while respecting the departmental mandate. The Terms of Reference for these governance committee assigns them the oversight and accountability with a well-defined scope, definition of key terms, as well as the roles and responsibilities of key stakeholders.

There was no multi-department governance committee to support the coordination of Securities process carried out by multiple departments. The Major Projects Deputy Ministers Committee (also known as the Resource Management Deputy Minister Committee) could provide the oversight on the risks associated with Securities to the GNWT once the Terms of Reference for the committee were approved.

Without assignment of a clear mandate on managing the GNWT risk associated with Securities handled by multiple departments, an “*Interim Departmental Protocol*” was established in 2014 at the time of devolution. A working group from Lands, ITI and ENR meets on regular basis to update the “*Interim Departmental Protocol*”. The temporary nature of the document allowed for on-going revisions. The March 2015 “*Interim Departmental Protocol*” was the most current document at the time of our audit (**Appendix B refers**). We noted that the “*Interim Departmental Protocol*” was ineffective in coordinating the management of Securities, in that:

- a. cash/cheque handling process, accounting for 45% of Securities transactions, had been well documented by Lands. However, the

detailed procedures were lacking in other departments involved in processing these transactions

- b. the direction on handling of Irrevocable Letters of Credit, that can range in value from \$25,000 to \$72 million, were not clear. For example; the list of authorized staff able to pick up the securities from Department of Finance Treasury has not been circulated
- c. there was no timeframe within which non-cash securities documents must be processed for the various transactions. While the Financial Administration Manual provides directions on the frequency of processing cash transaction, similar direction was not provided for non-cash securities. For example: there was no stipulated time frame within which department staff should deliver the Securities to Finance Treasury
- d. There was no protocol to track, capture and monitor the GNWT risks related to the Securities. The SharePoint used to track Securities by LFA Division only recorded the amount of legally required Securities to be held by the GNWT. However, the estimate of Securities required can vary based on:
 - i. assessment done by the department during the review process
 - ii. proposal submitted by the project developer
 - iii. recommendation of the Land and Water Board based on the presentations by GNWT and the project proponent
 - iv. agreed upon by the Minister of ENR on behalf of the GNWT.

For example: The SharePoint showed that \$11.7 million was held as Securities for the project proposed by Northern American Tungsten Corporation Can-Tung Mine (Can-Tung Mine). However, there was range of values assigned to the risk:

Description		Amount (in millions)
a	Security estimate by the GNWT department	\$42.0
b	Can-Tung Mine project proposal	\$15.0
c	Land & Water Board Security approved amount	\$31.0
d	Security per ENR Minister's agreement	\$31.0

The “*Interim Departmental Protocol*” served was a reasonable tool to support the coordination of Securities when the GNWT assumed responsibility for Securities. However, it did not develop to become the established authoritative standard in providing directions to internal and external stakeholders to mitigate the GNWT Securities risks.

Risk Profile:

Risk Level of Observation:	High risk based on 50% to 75% likelihood, impact requires detailed research and management planning by Senior Management.
Risk Responsibility	Deputy Minister, Lands
Risk Mitigation Support:	<ul style="list-style-type: none"> • Deputy Minister, ENR • Deputy Minister, Finance • Deputy Minister, ITI • Deputy Minister, Justice • Director, LFA Division, Lands

Recommendation

We recommend that to manage the GNWT Securities risks:

- a) a multi-departmental governance committee be established to provide oversight, transparency and accountability to coordinate the management of Securities
- b) under the guidance of governance committee, the March 2015 “*Interim Departmental Protocol*” be modified and approved to provide clear authoritative guidance to all internal and external stakeholders.

2. SharePoint Spreadsheet Securities Data

Observation

The use of SharePoint spreadsheet to accurately track over \$500 million in Securities was not sustainable over a period of time.

One of the purposes of the Interim Protocol was to “*integrate the process to provide reliable information to all departments involved for both operational and reporting requirements*” (**Appendix B refers**).

The SharePoint spreadsheet used by Finance during the devolution of Securities from AANDC to GNWT was subsequently used by the LFA Division to track these Securities. Digital Integrated Information Management System (DIIMS) used in Lands was not considered for tracking purposes in April 2014 as not all the key stakeholders had access to that tool.

The volume of transactions through the SharePoint spreadsheet was less than 200 items; the dollar value exceeded \$500 million. Our review of SharePoint spreadsheet showed that:

- the information was incomplete as indicated by missing information in the following fields:

Field Name	Missing data
Security deposit number	21 of 90 listed items
Issue authority	21 of 90 listed items
Date Cheque/cash received	45 of 60 listed items

- incorrect information was recorded in specified fields: in examining 159 Securities, we noted that incorrect data was recorded in the specified spreadsheet field:

Specified Field	Actual data recorded
Project Location	Licence number for 25 securities instead of project location
Region	“ <i>Test Region 1</i> ” for 21 securities rather than name of region

- “key fields” required for tracking of Security were not set-up as required fields in the spreadsheet. For example, fields like “*value of security*” and “*form of security*” would be “key fields” for tracking of

Securities. However, as these fields were not required fields, the information related to Securities was omitted in some cases.

An unexplained system malfunction was identified during our review of the SharePoint spreadsheet. SharePoint reported information in the “*project location*” field inconsistently depending on whether the user was in “*edit*” or “*view*” mode. The likelihood of SharePoint error increased because users had access to “*Datasheet mode*” of processing. This function switches the display from single line items to the entire list (i.e. in Excel spreadsheet mode), which allows the 22 users with “*edit*” access to make mass changes to the data intentionally or accidentally.

Staff members made multiple reviews of the spreadsheet data as a result of unexplained system malfunction and the issues around incomplete and inaccurate data. While the spreadsheet data integrity of Securities data was not high, we did not find any material error in the dollar value recorded in the spreadsheet. The Lands Finance Section had implemented a compensating internal control on the total valuation of Securities. A three-way reconciliation to assess the reasonableness of the amount recorded in SharePoint was performed on regular basis. The reconciliation matched the information in SharePoint to Land Information Management System and the cash portion of SharePoint to System of Accountability and Management.

The main causes of the data integrity were:

- lack of governance framework to standardized data entry requirements
- the manner in which SharePoint was configured did not make key fields mandatory
- SharePoint spreadsheet had many of the inherent weaknesses of any spreadsheet such as editing of data without an audit trail.

The overall impact of weak SharePoint controls was unreliable information for reporting purposes, risk of mass data corruption, and inefficient use of staff time for data reviews aimed at detecting accidental or intentional errors was well recognized by Lands.

In January 2015, FMB approved the Lands proposal to allocate \$275,000 funding for development and acquisition of a Security Administration and Processing System (**Appendix C refers**). By April 2015, all the departments involved in processing and reviewing information on the SharePoint spreadsheet had access to DIIMS.

Risk Profile:

Risk Level of Observation:	Medium risk based on 50% to 75% likelihood, impact requires specific allocation of management responsibility.
Risk Responsibility	Deputy Minister
Risk Mitigation Support:	<ul style="list-style-type: none">• Assistant Comptroller General, Finance• Executive Director, Informatics Shared Services ENR/ITI/Lands• Director, LFA Division, Lands

Recommendation

We recommend, prior to developing a new software application for Securities:

- a) that a governance framework around the ownership, accountability and responsibility of Securities data be documented
- b) that data integrity in the existing spreadsheet be enhanced by edit validation rules and audit trail
- c) that the current data in the SharePoint spreadsheet should be reviewed and corrected
- d) that a survey of Canadian jurisdictions holding Securities be done as a first step in the “fit-gap” analysis to develop and design a system that meets the GNWT requirements.

Management Response:

Action Plan	Completion Date
<p>a. Lands is working with all affected departments to confirm and document appropriate procedures and responsibilities for handling securities documents and maintaining accurate and complete security document data.</p>	<p>December, 2016</p>
<p>b. The SharePoint site is owned by the Department of Finance and was developed by them as a document registry, not a securities management system. Addition of validation and edit rules would require their cooperation.</p>	<p>December, 2016</p>
<p>Data integrity among other things will be dealt with in the new SAPS project approved in 2015-16 and included in the capital carry-overs for 2016-17.</p>	<p>Recommended action has been completed.</p>
<p>c. The Departments of Lands and ENR completed a review of and updating of the data in the SharePoint site in the summer of 2015. There are few securities transactions and because staff are more familiar with the process, the likelihood of significant new missing or incorrect data at this time is remote.</p>	<p>Recommended action has been completed.</p>
<p>d. The Department engaged IAG Consultants to conduct a survey of Canadian jurisdictions holding securities. The report dated November 24, 2015, concluded that “Of the ten jurisdictions scanned there were none that deployed a technical solution (either commercially available or internally developed) that sufficiently covered the proposed requirements the GNWT identified for their Security Administration and Processing System.”</p>	<p>Recommended action has been completed.</p>

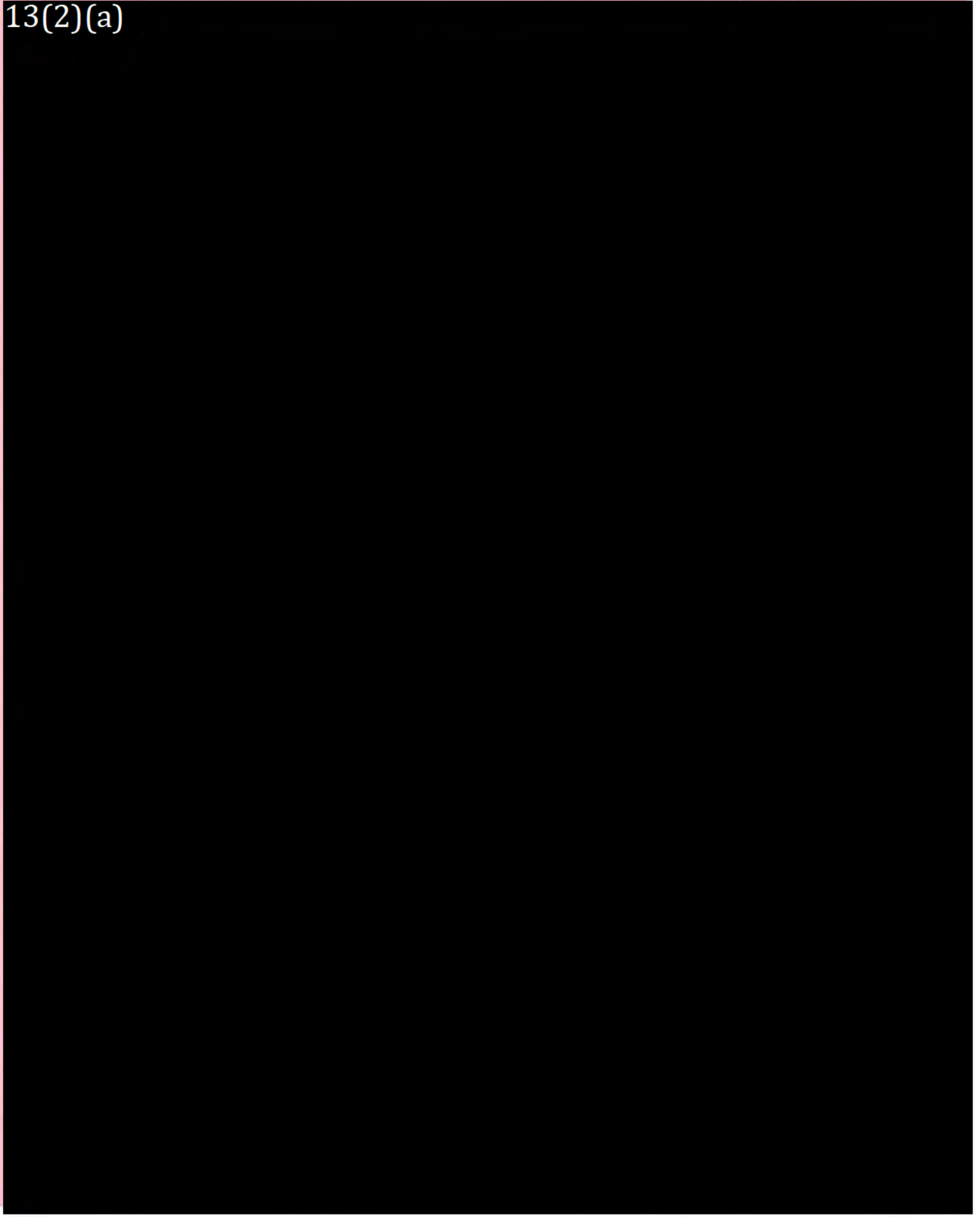
E. ACKNOWLEDGEMENT

We would like to thank the staff in Lands for their assistance and cooperation during the audit.

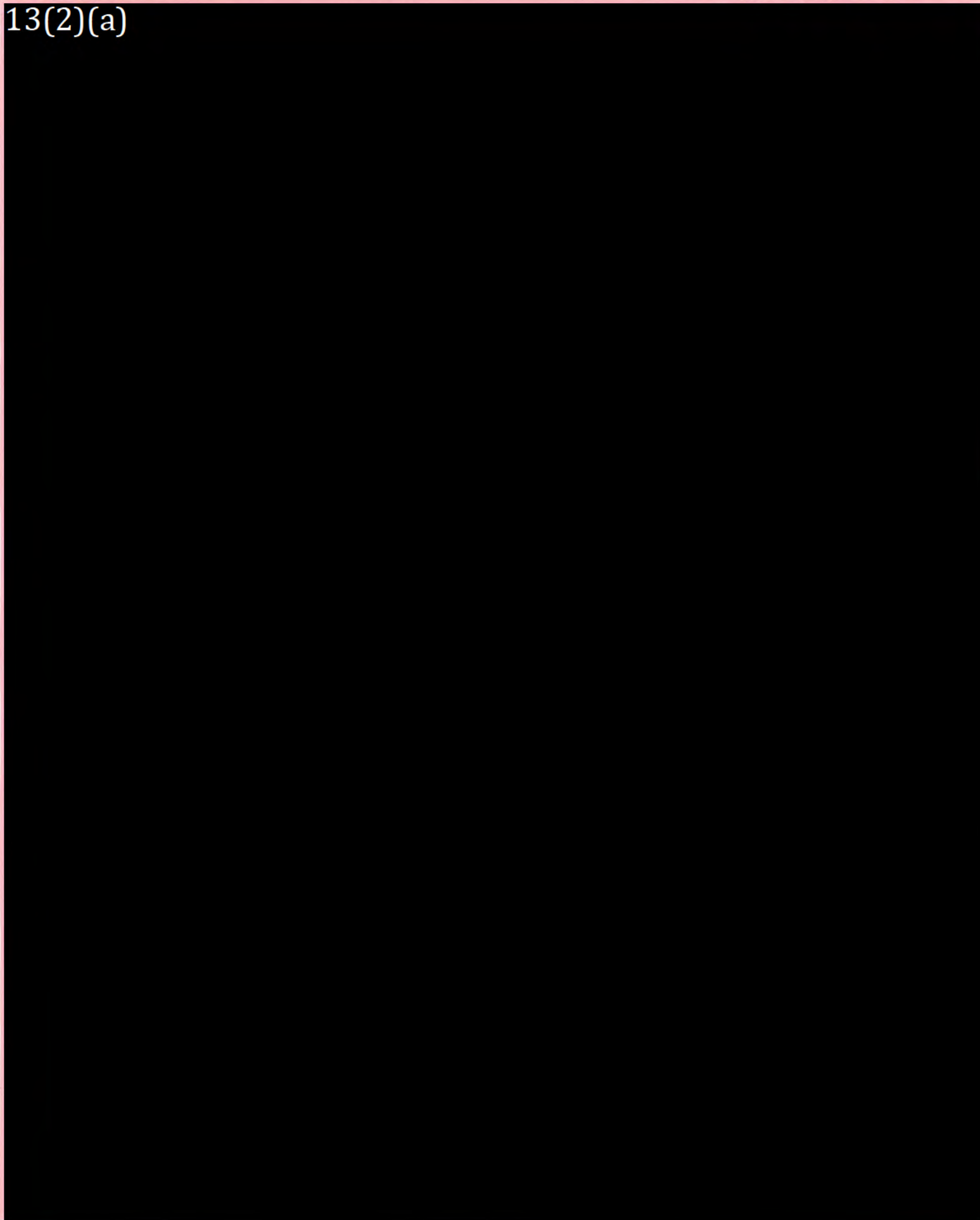
A handwritten signature in black ink, appearing to read 'T. Bob Shahi', written in a cursive style.

T. Bob Shahi
Director


13(2)(a)




13(2)(a)



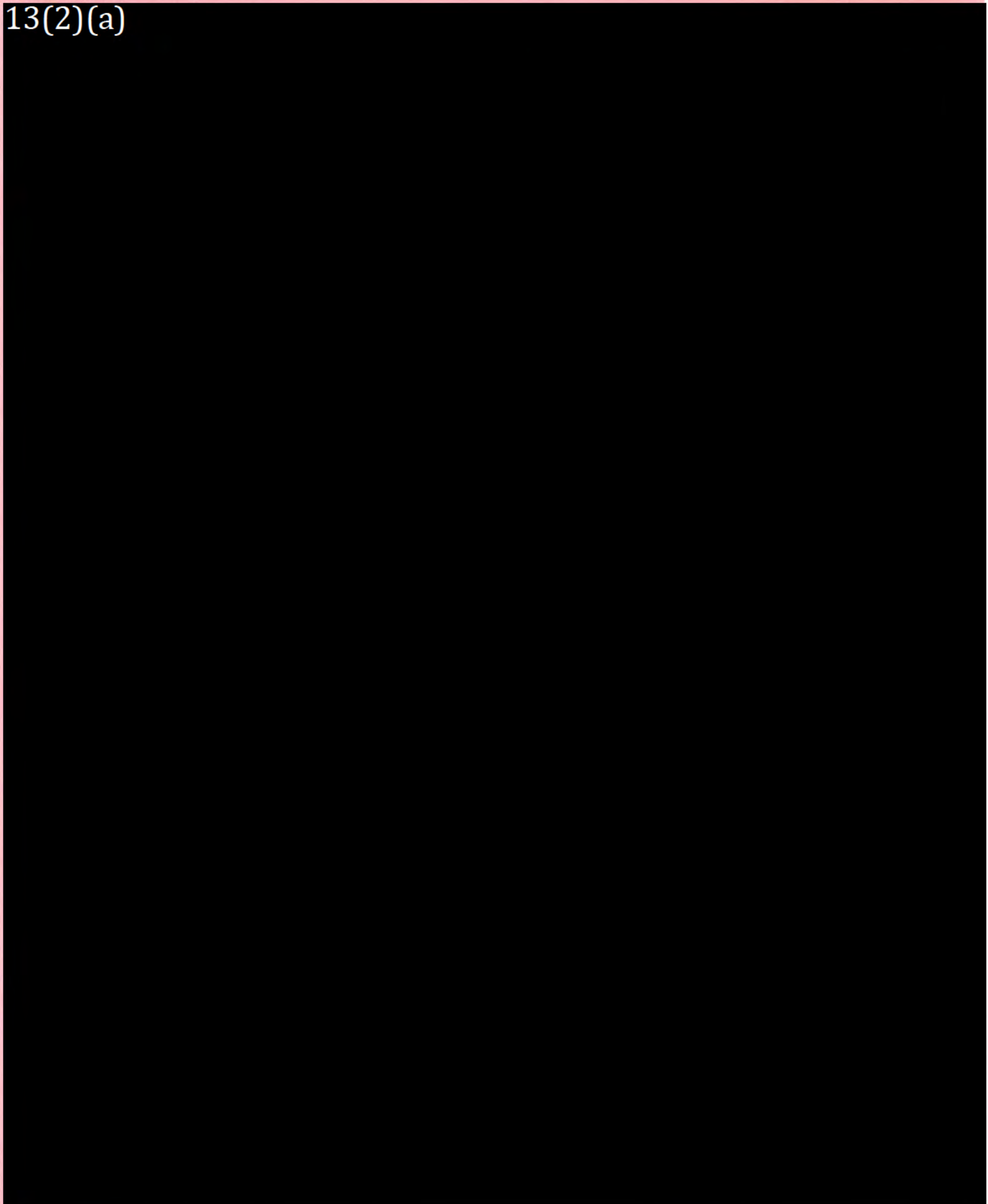
13(2)(a)



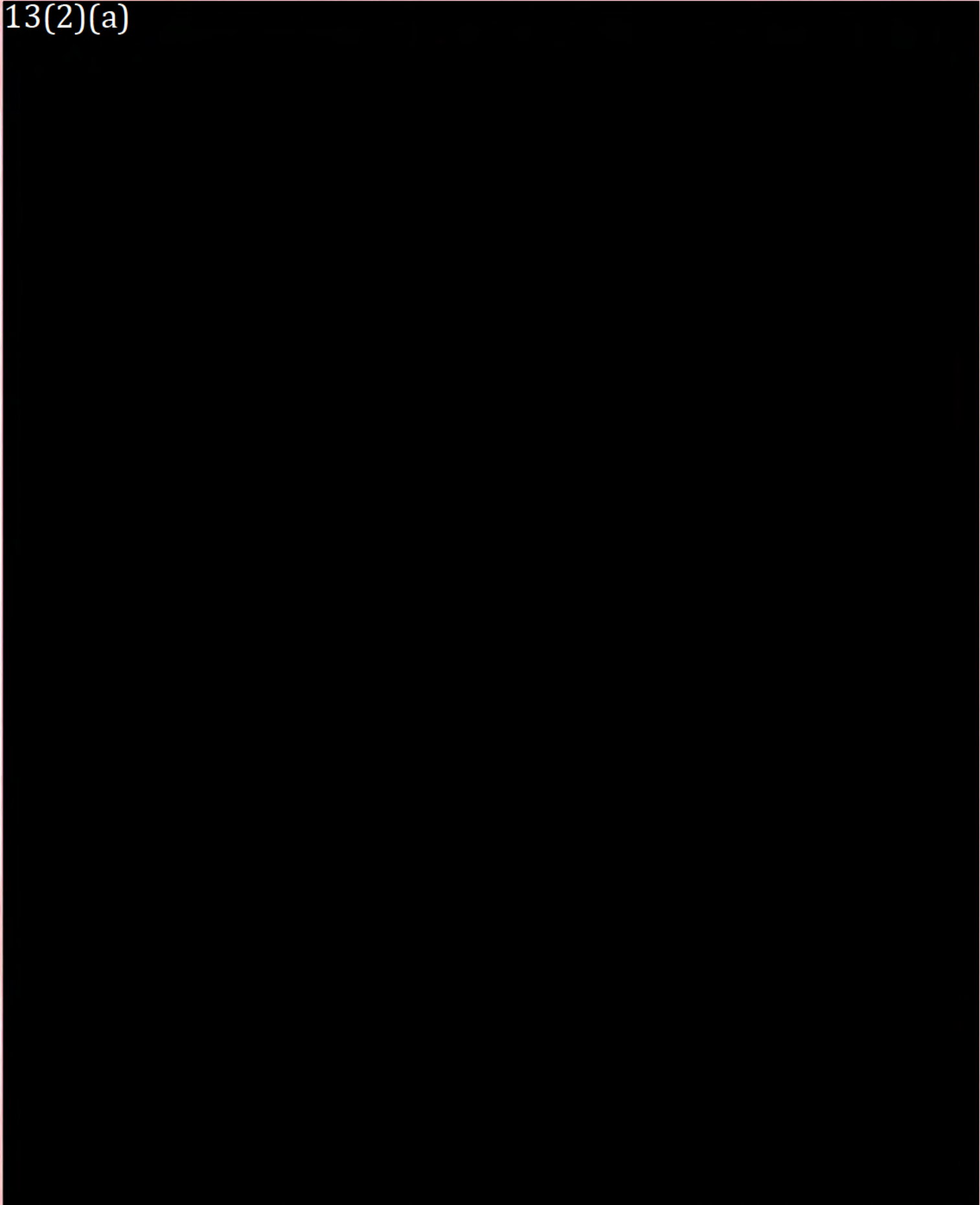
13(2)(a)



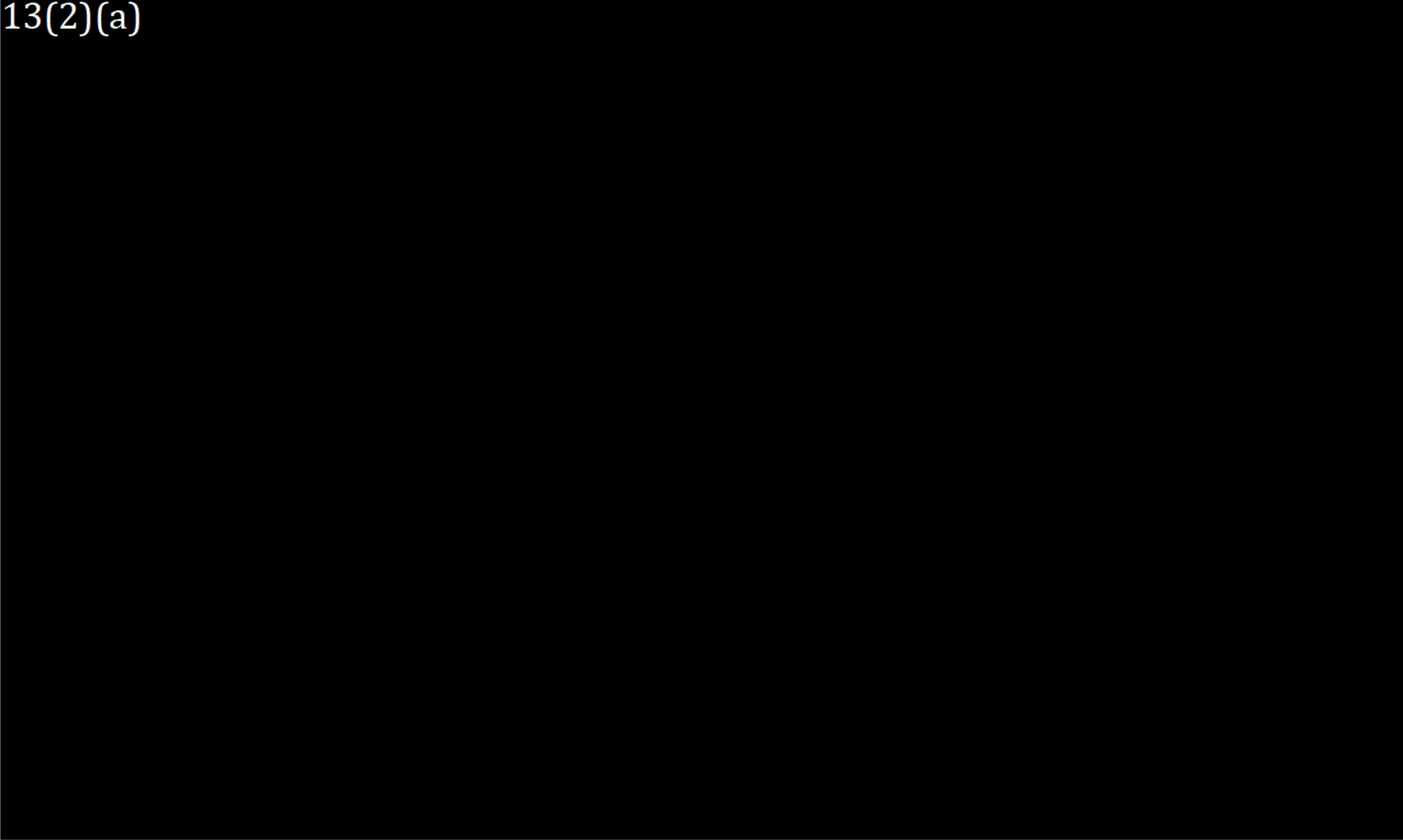
13(2)(a)



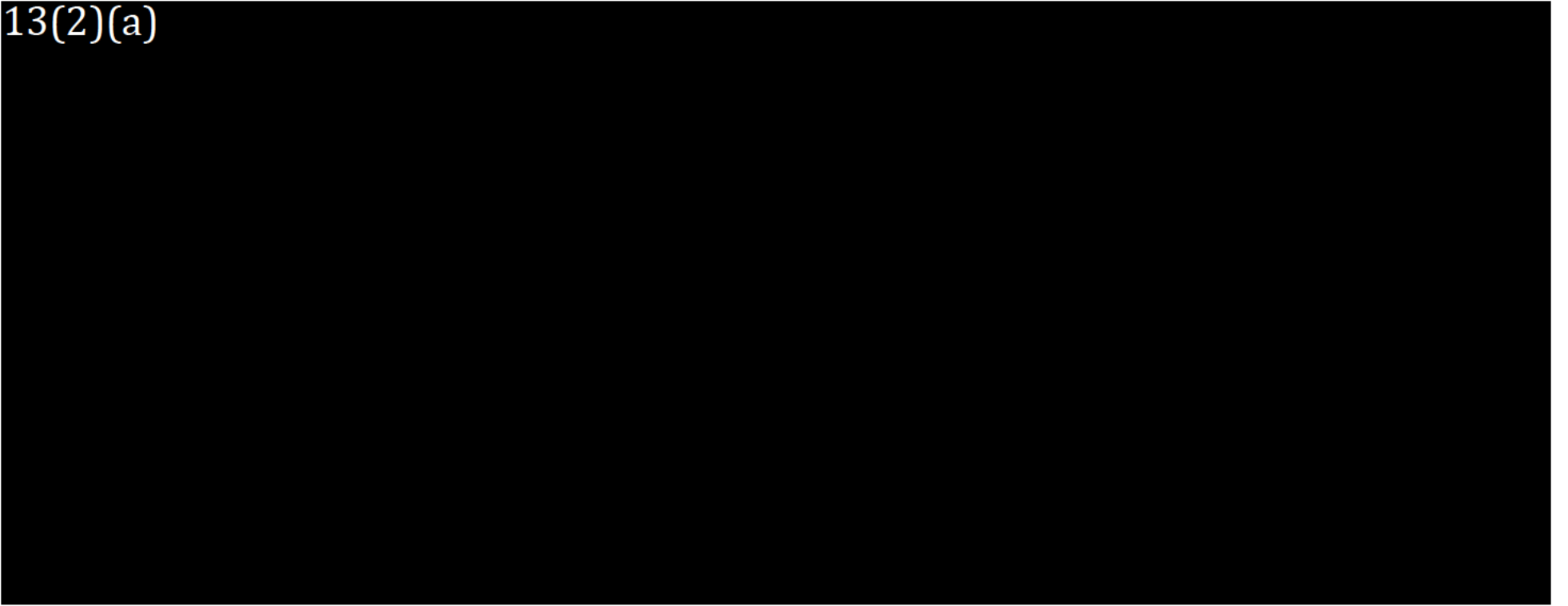
13(2)(a)



13(2)(a)



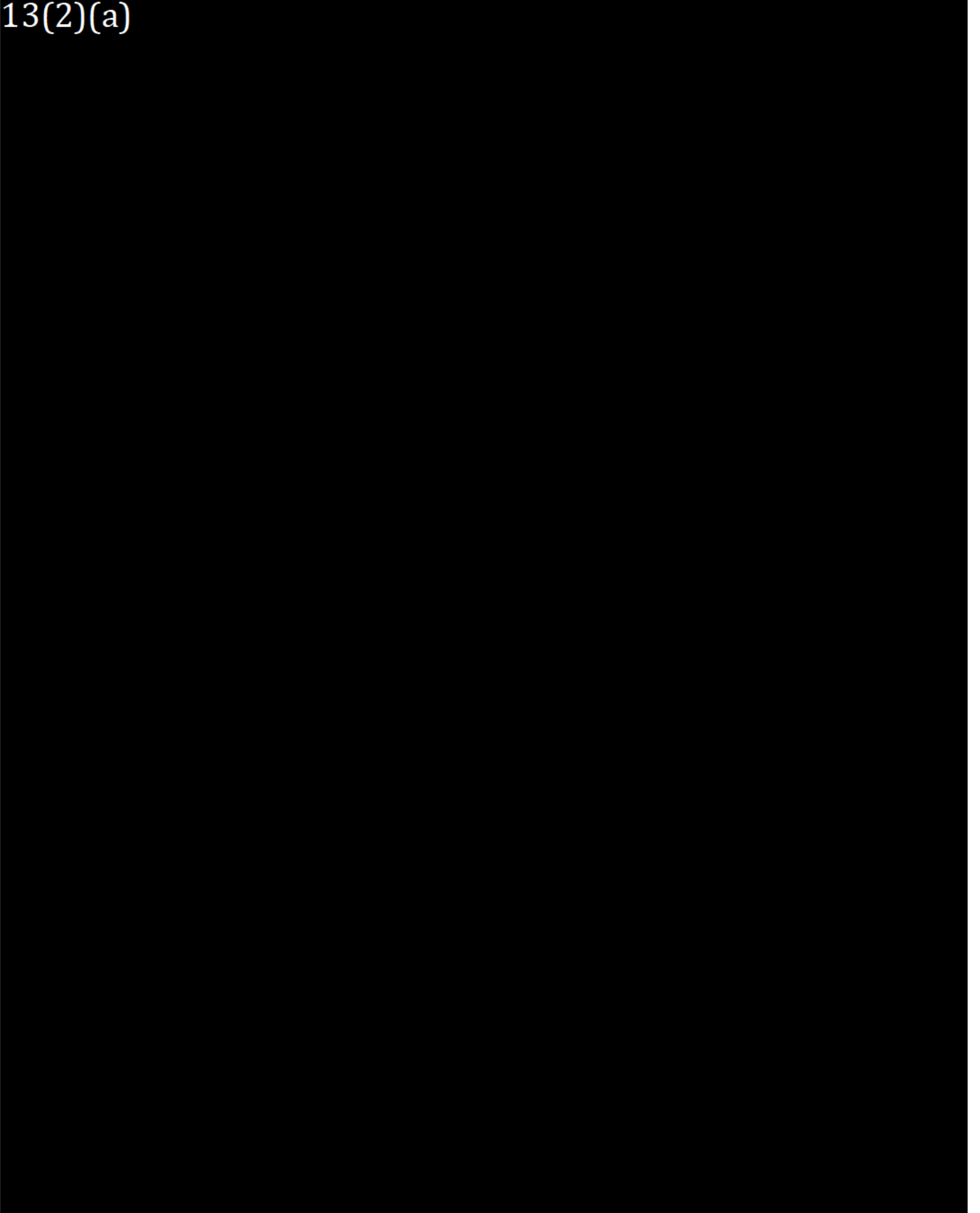
13(2)(a)



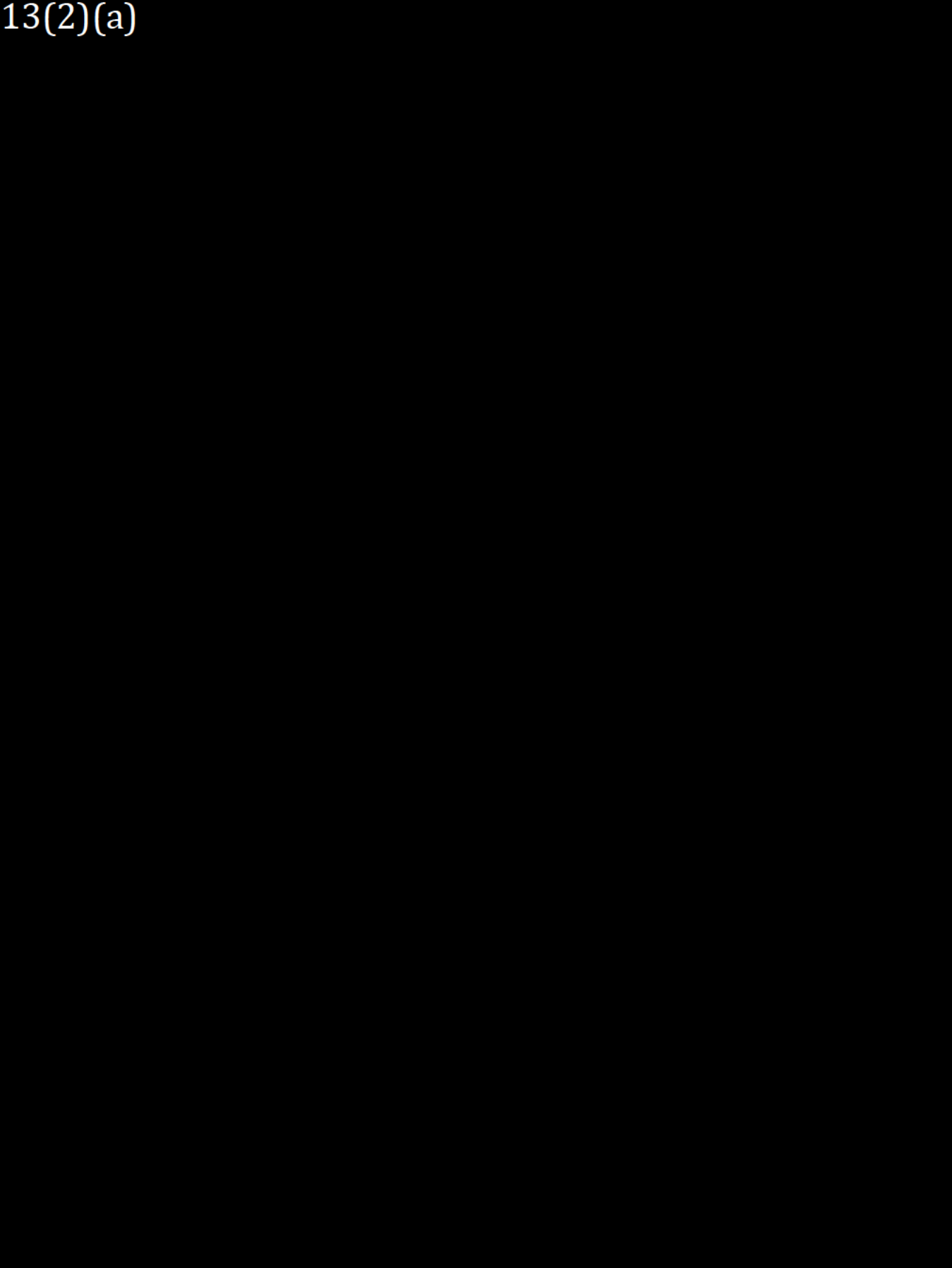
APPENDIX A

Confidential

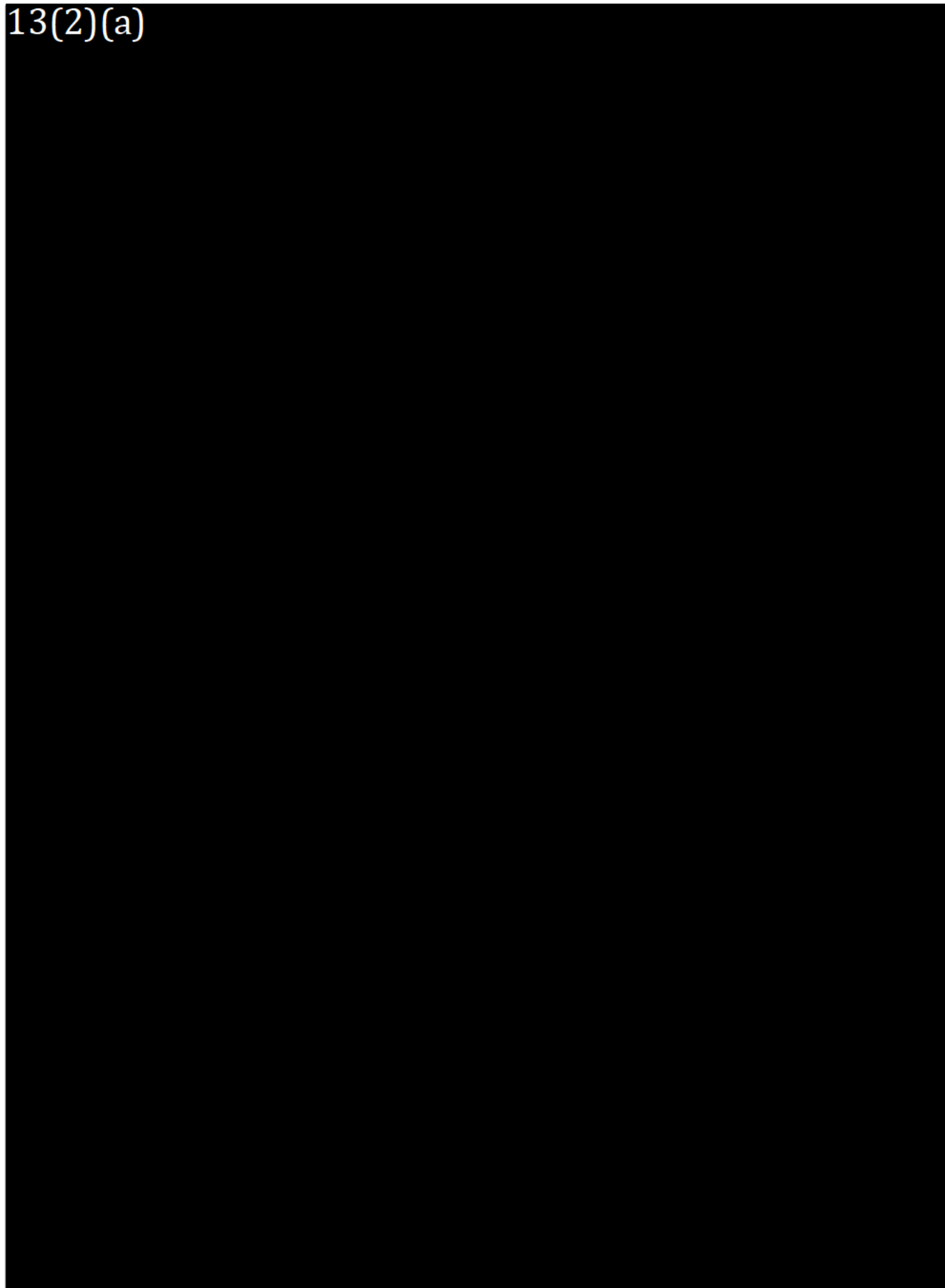
13(2)(a)



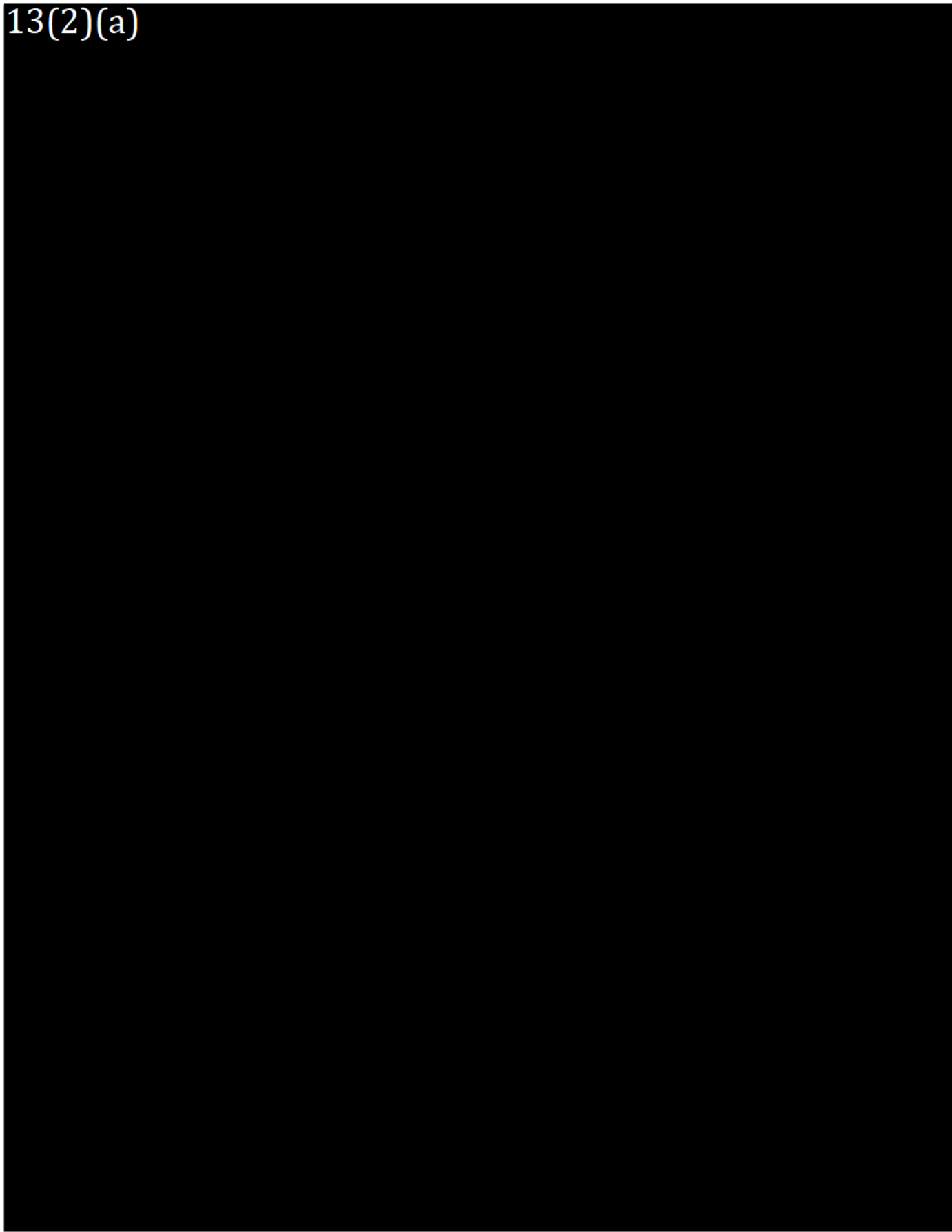
13(2)(a)



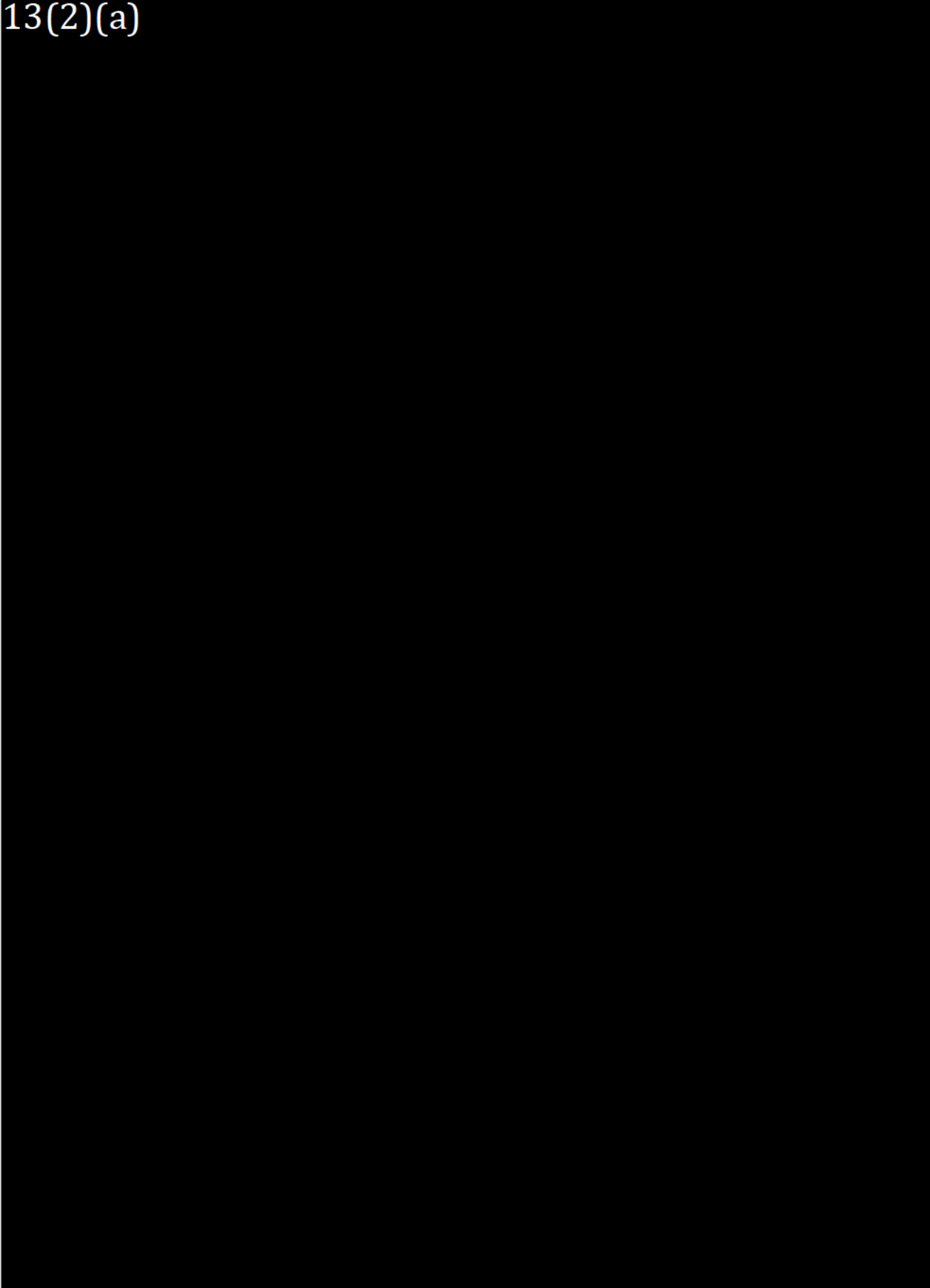
13(2)(a)



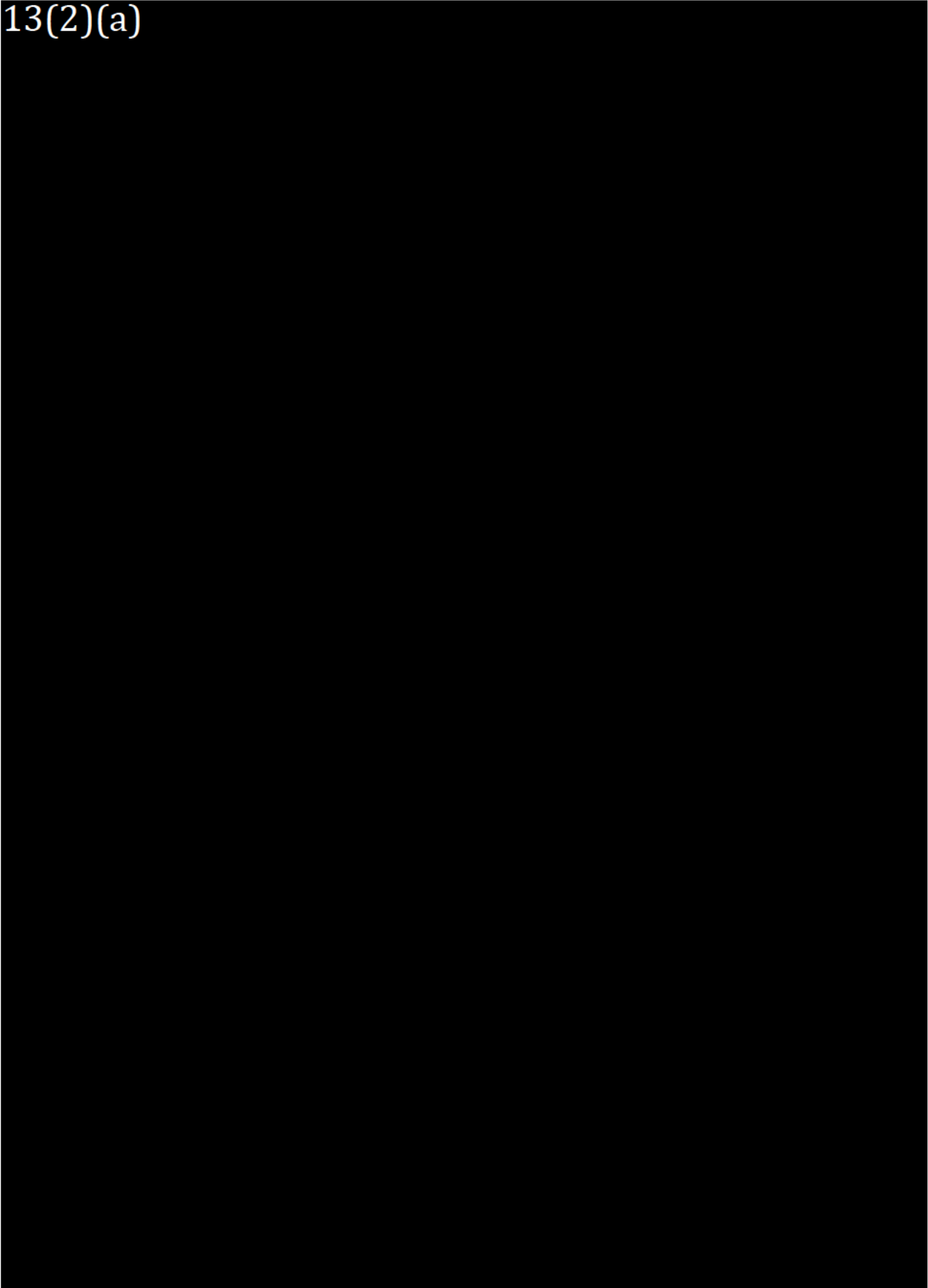
13(2)(a)



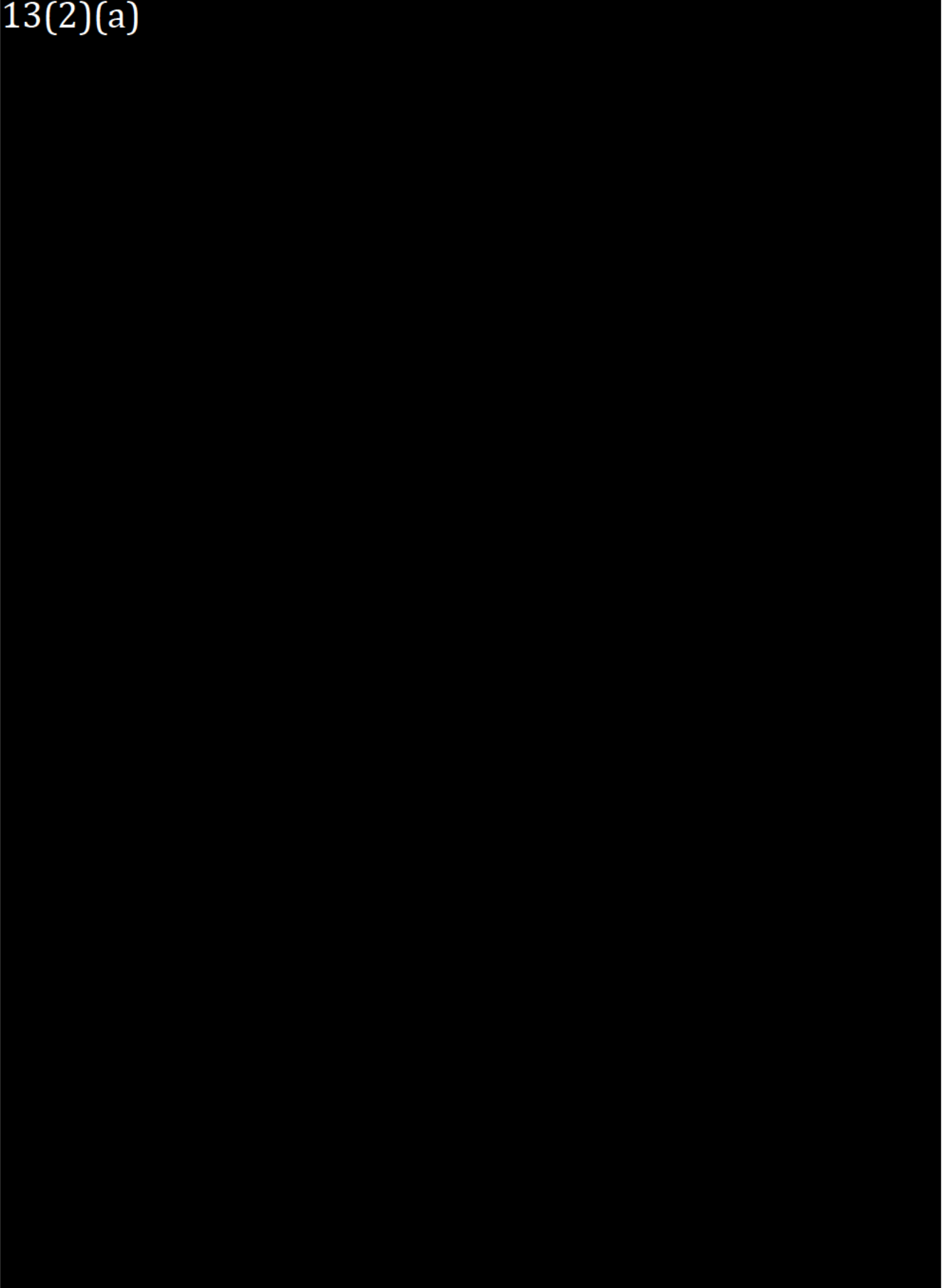
13(2)(a)



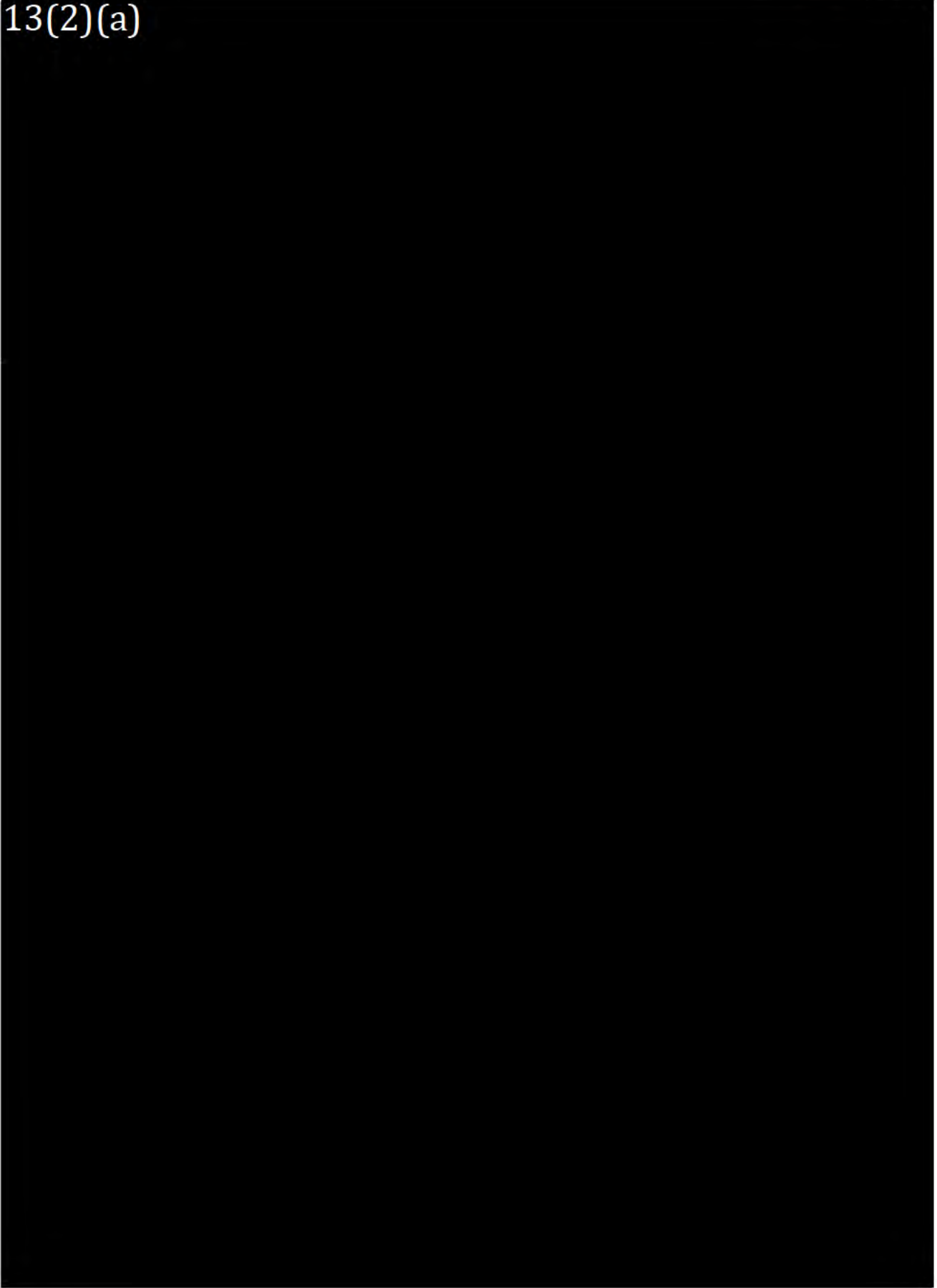
13(2)(a)



13(2)(a)



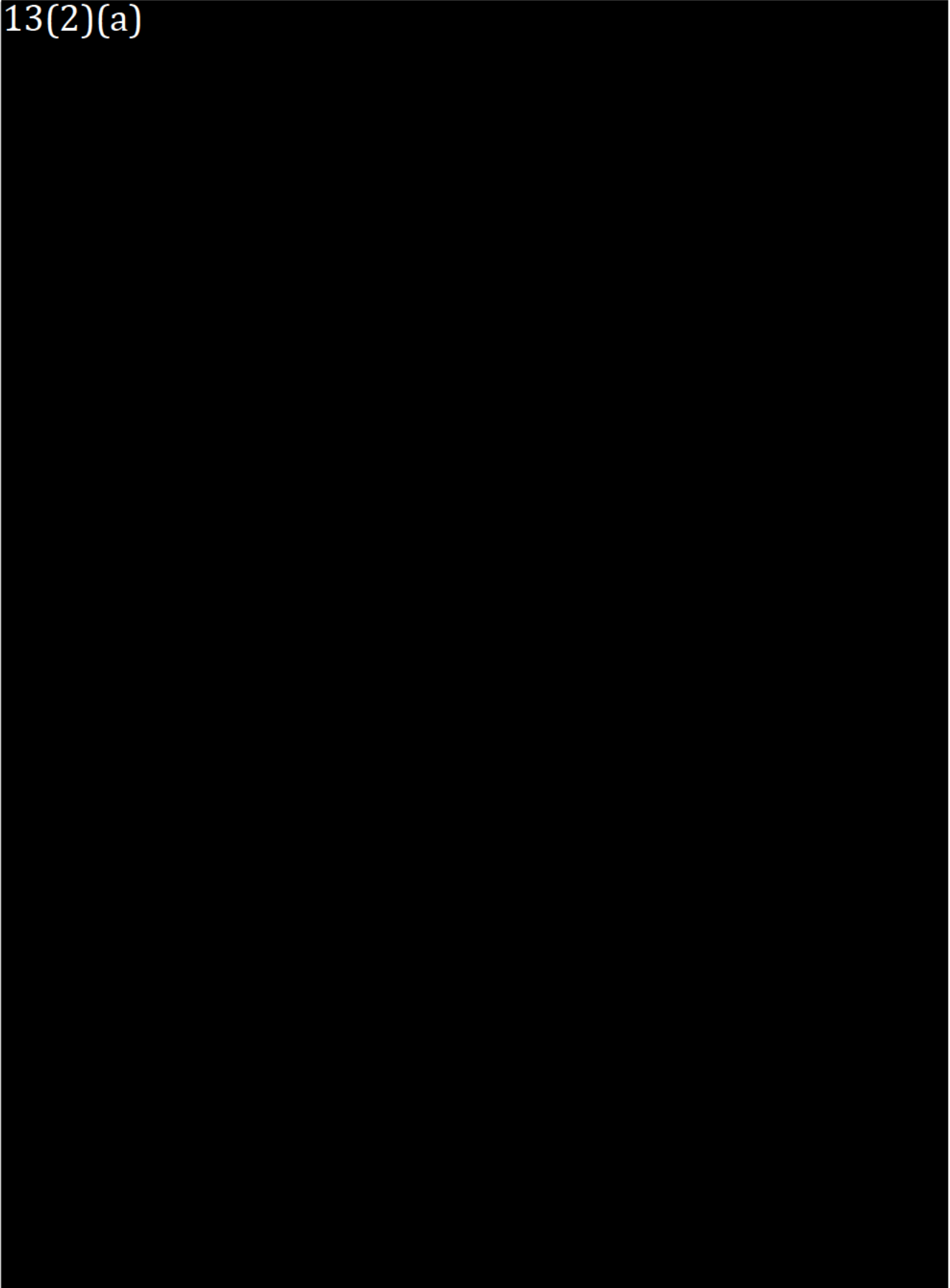
13(2)(a)



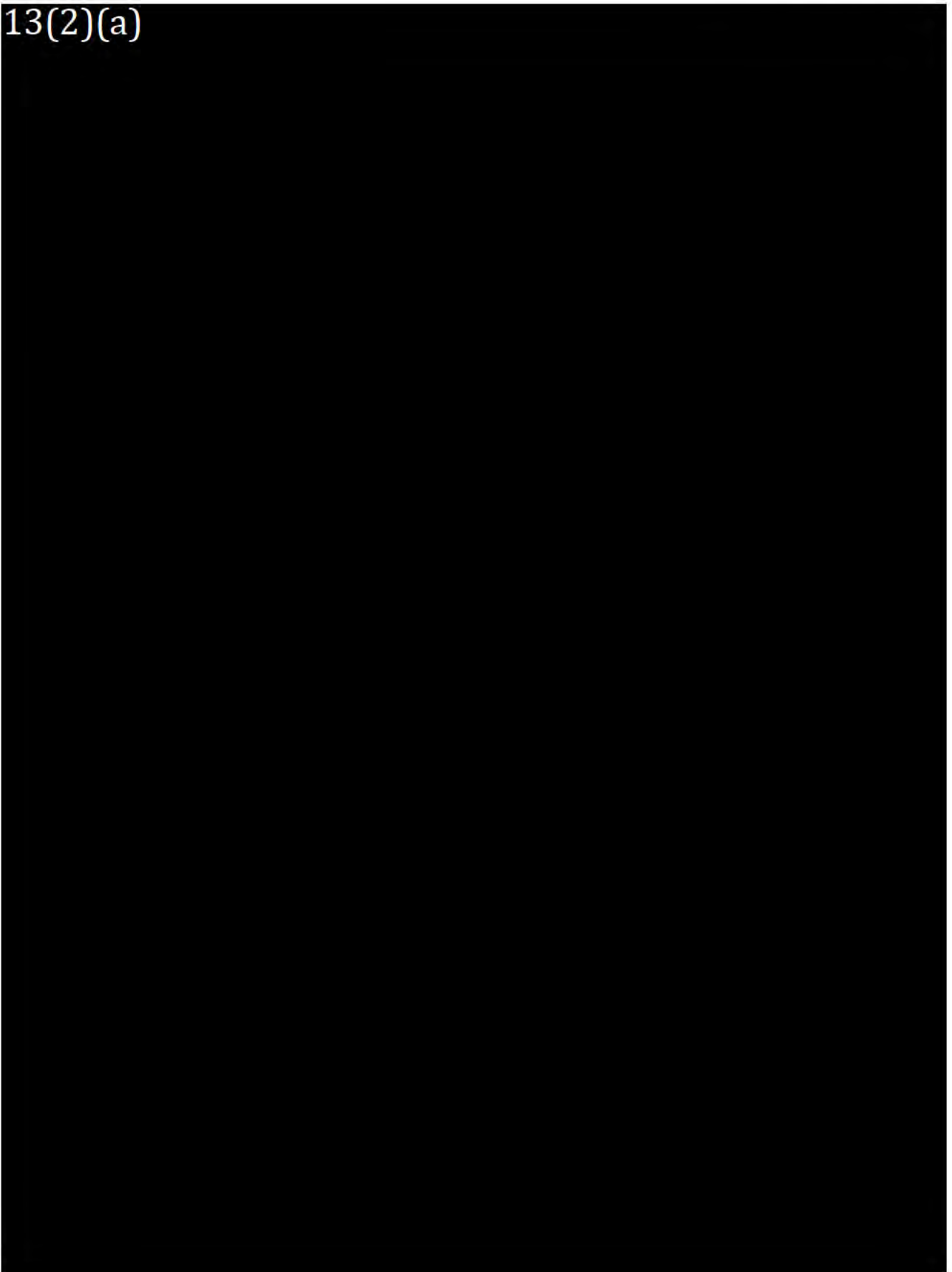
13(2)(a)



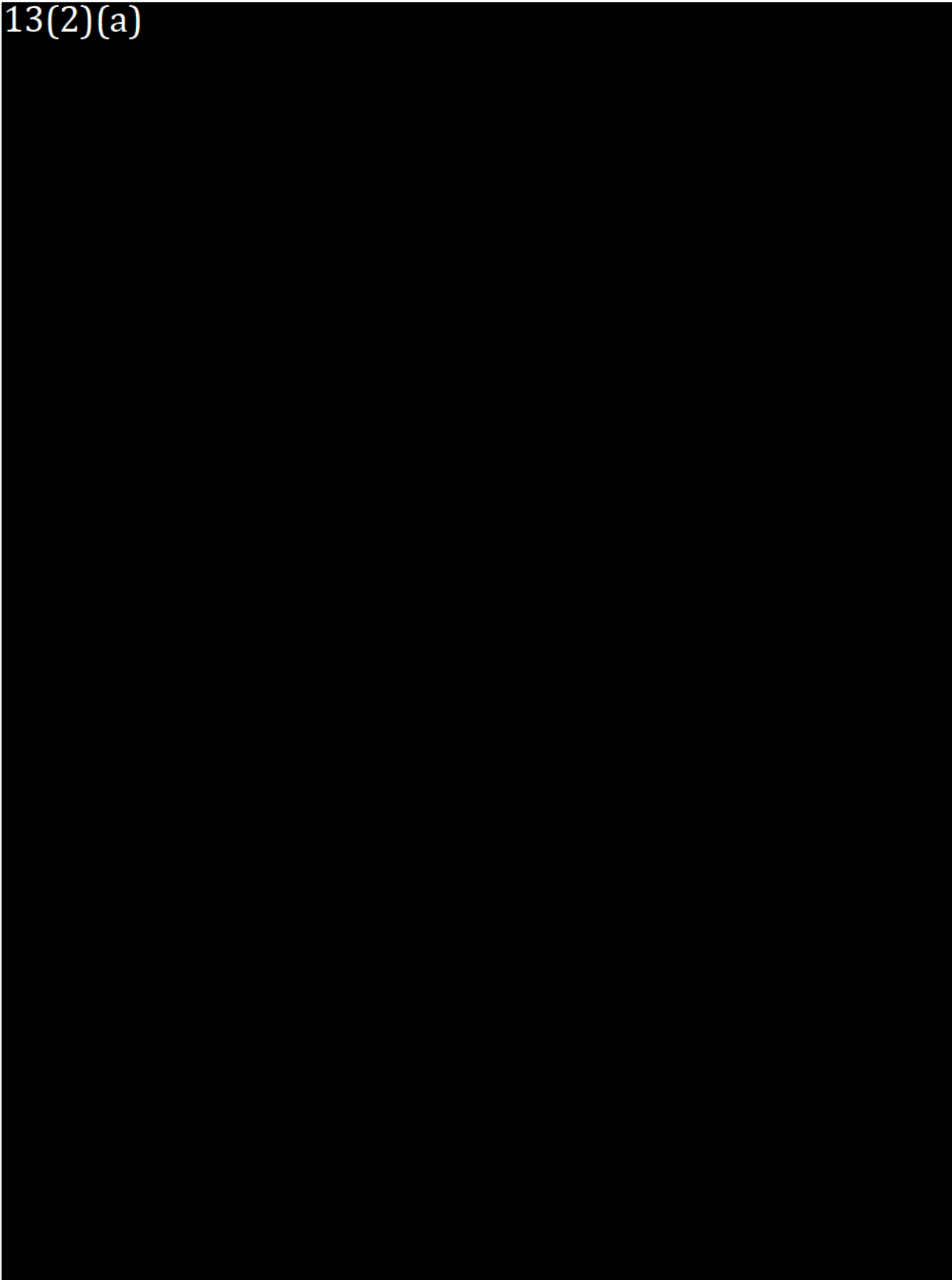
13(2)(a)



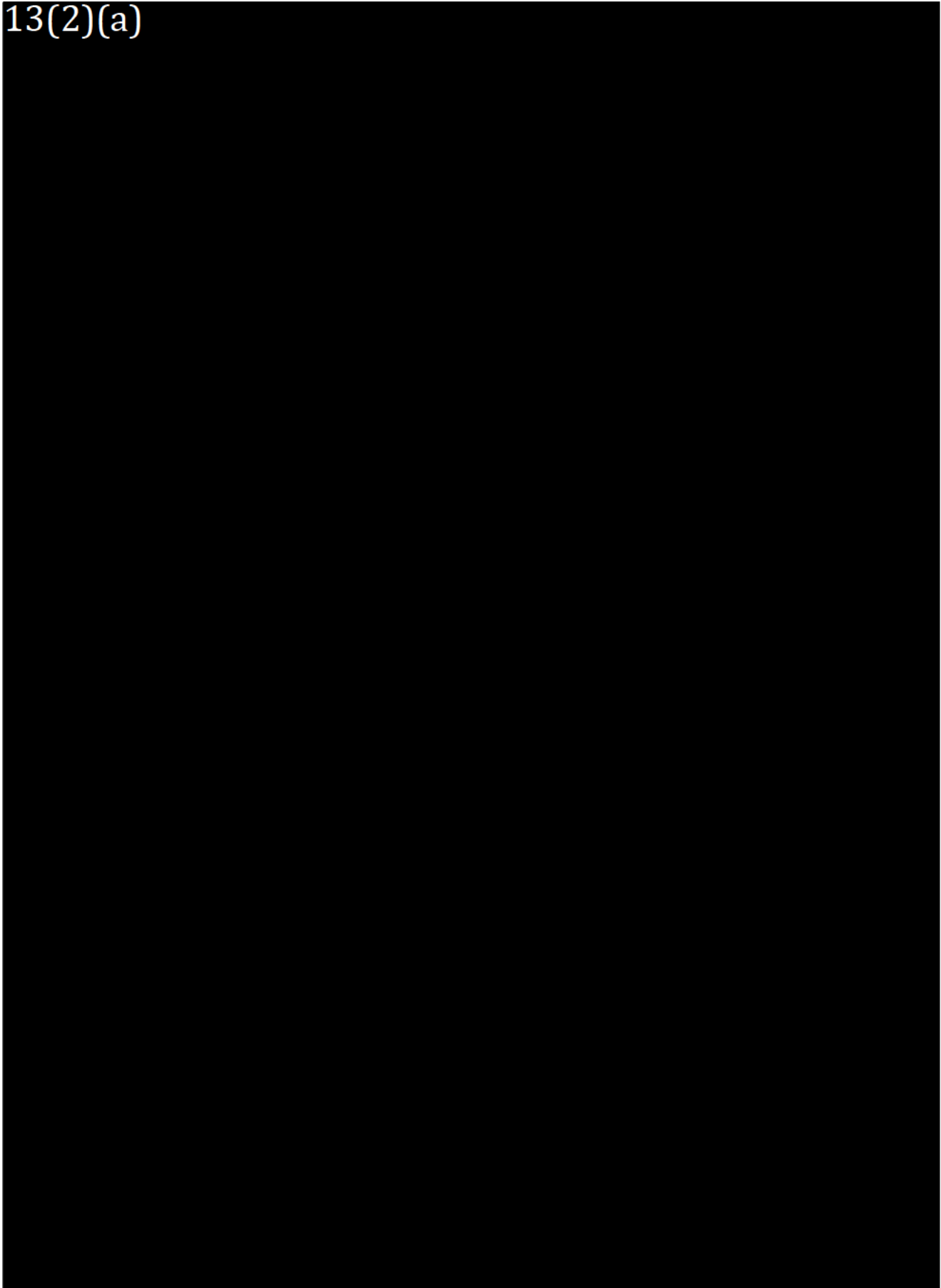
13(2)(a)



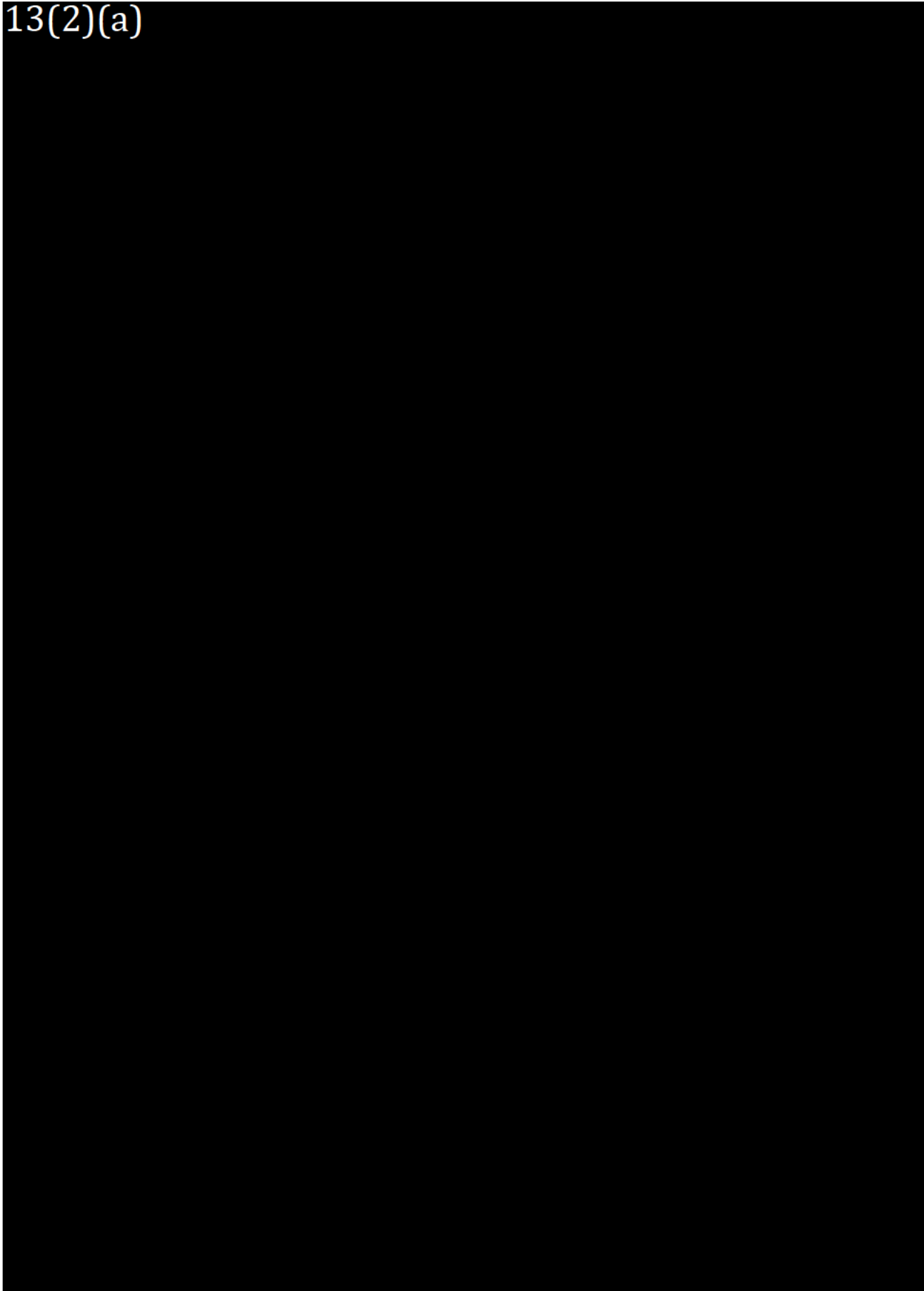
13(2)(a)



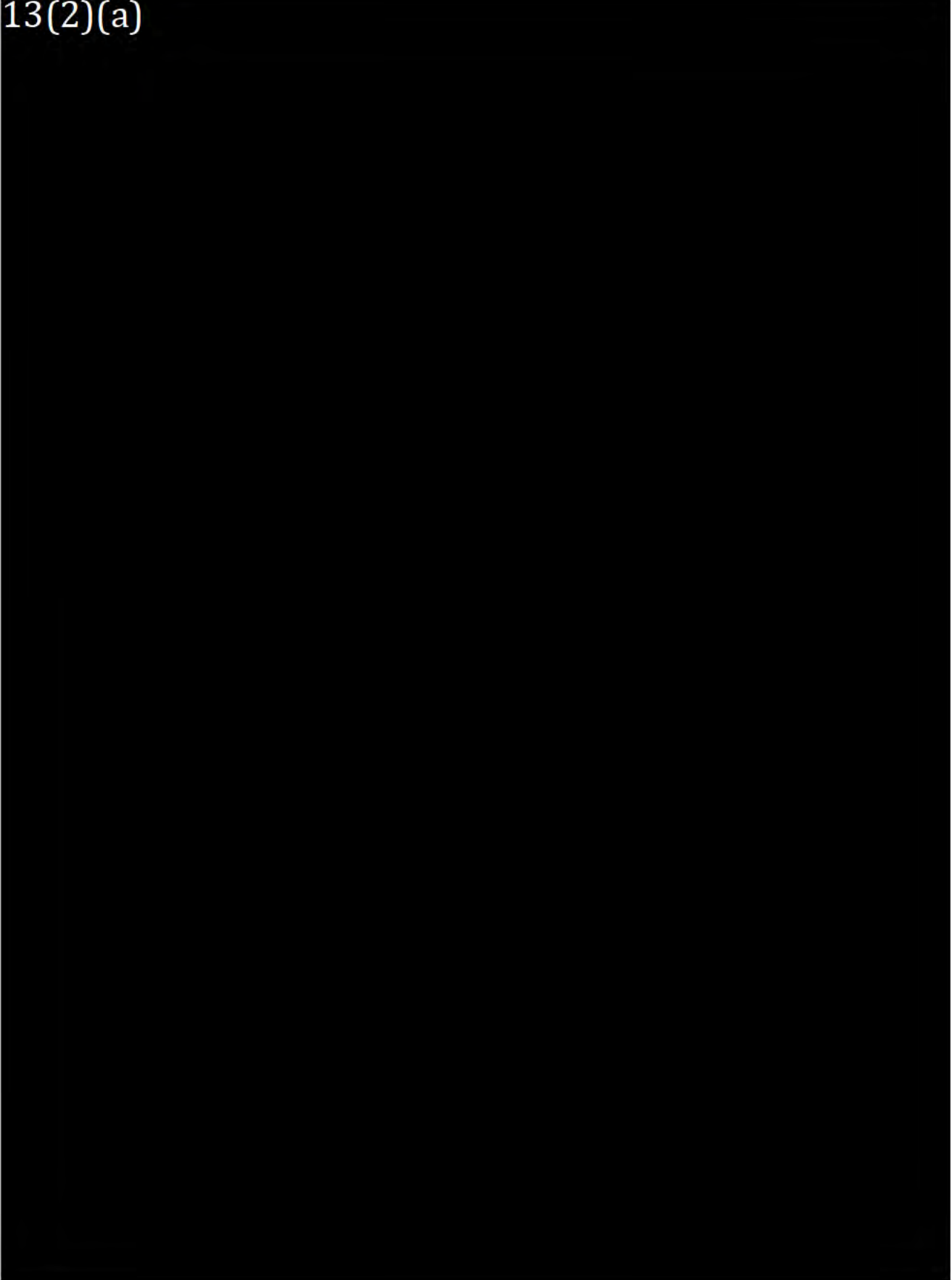
13(2)(a)



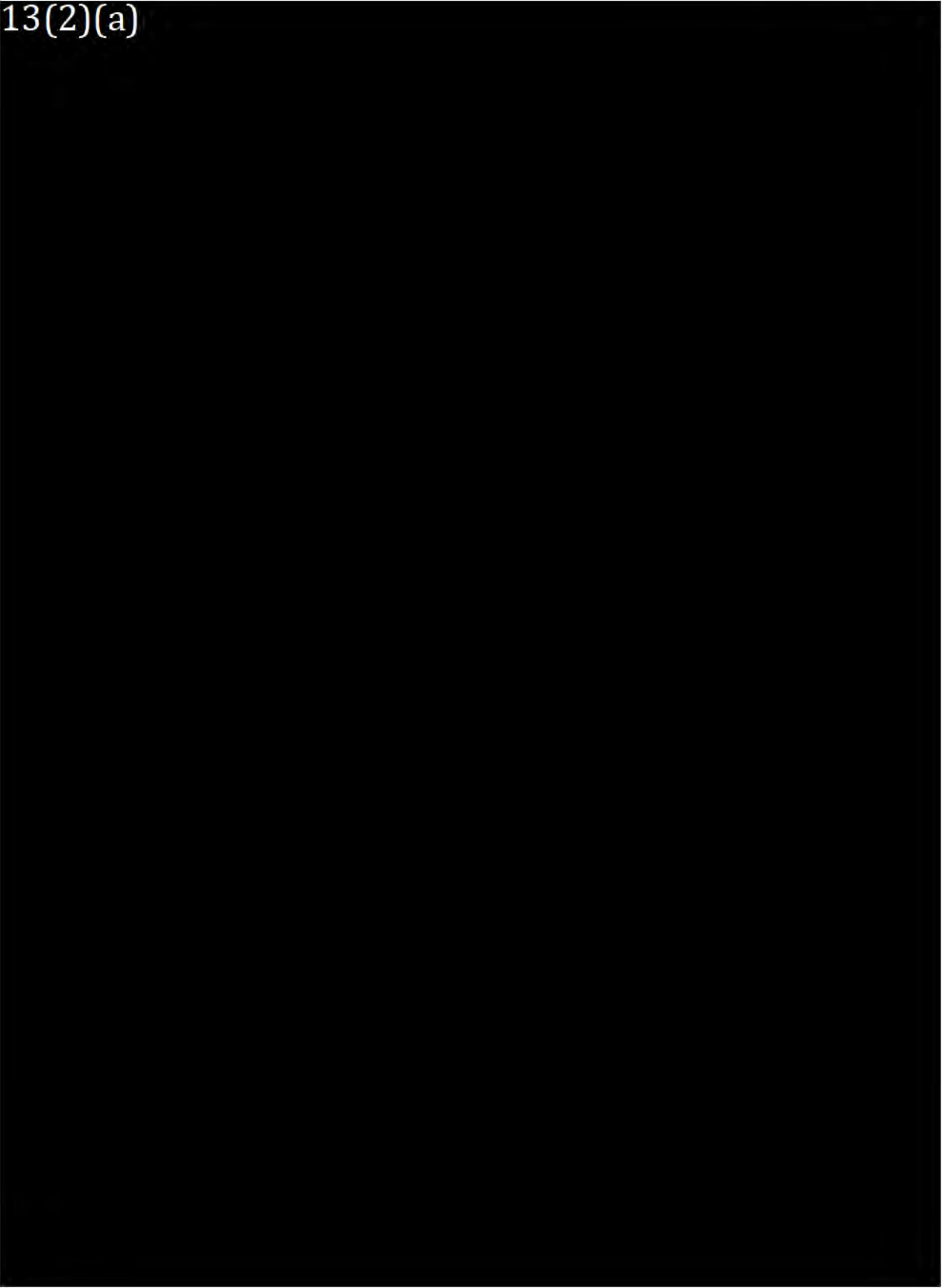
13(2)(a)



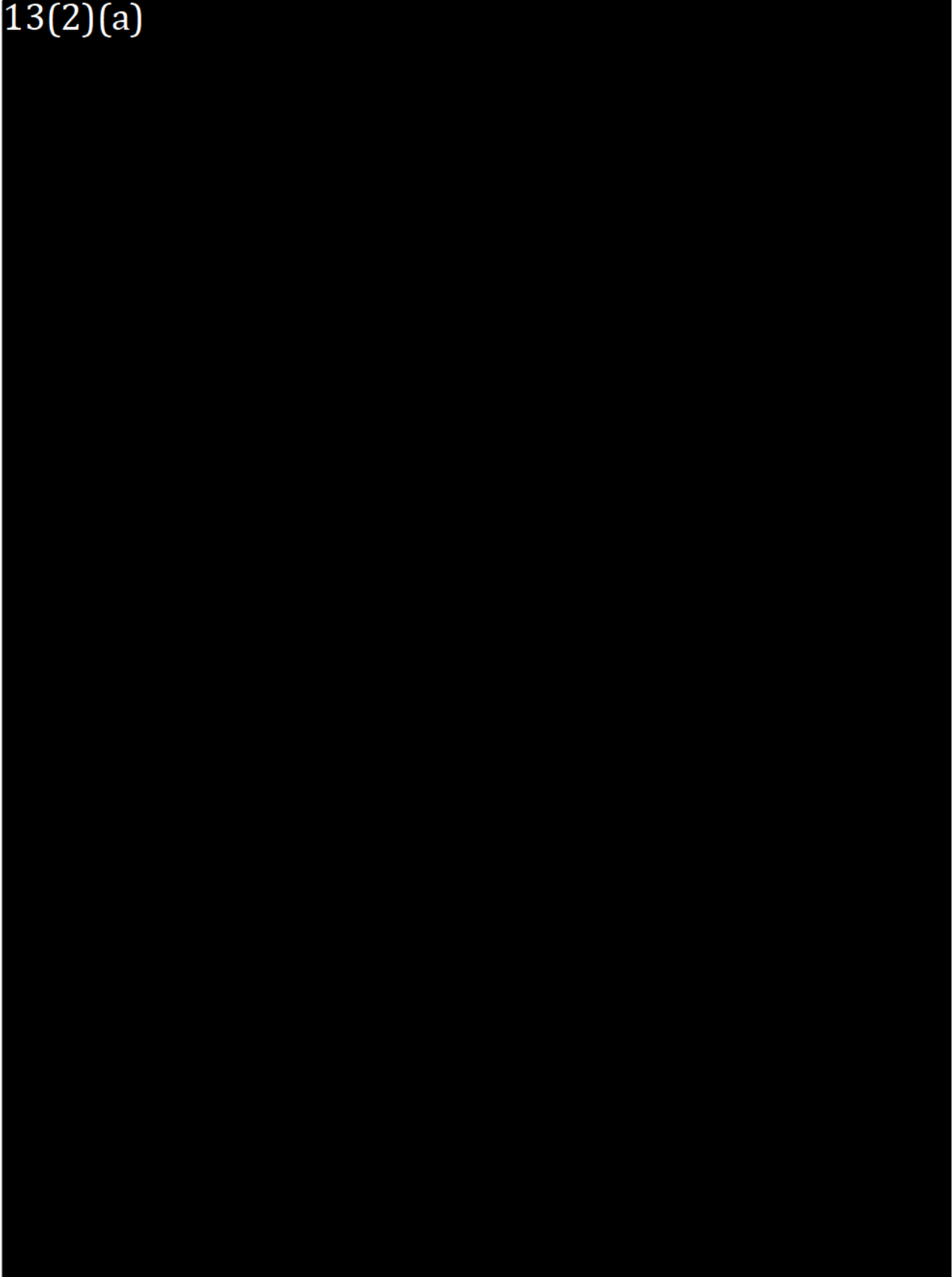
13(2)(a)



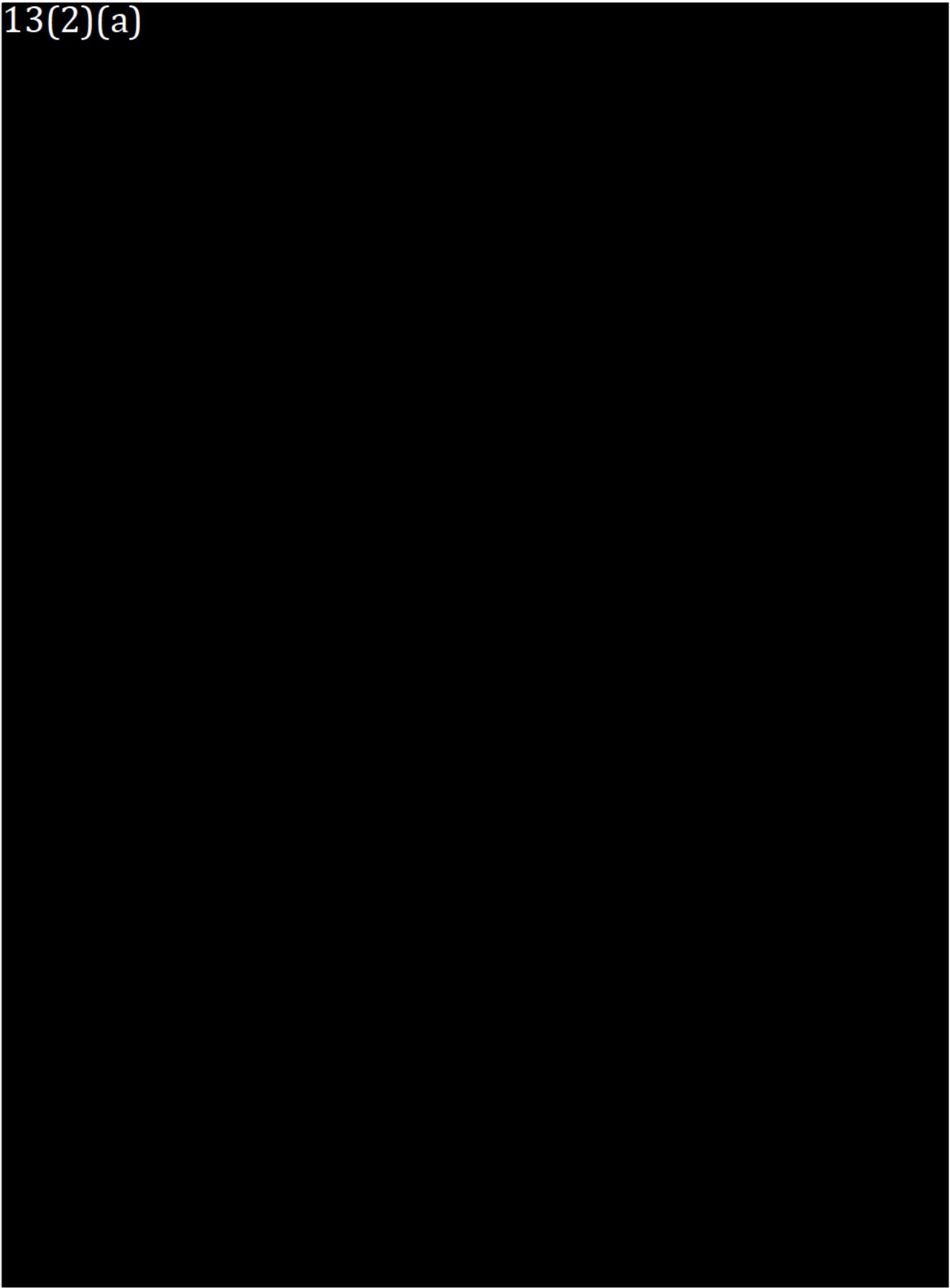
13(2)(a)



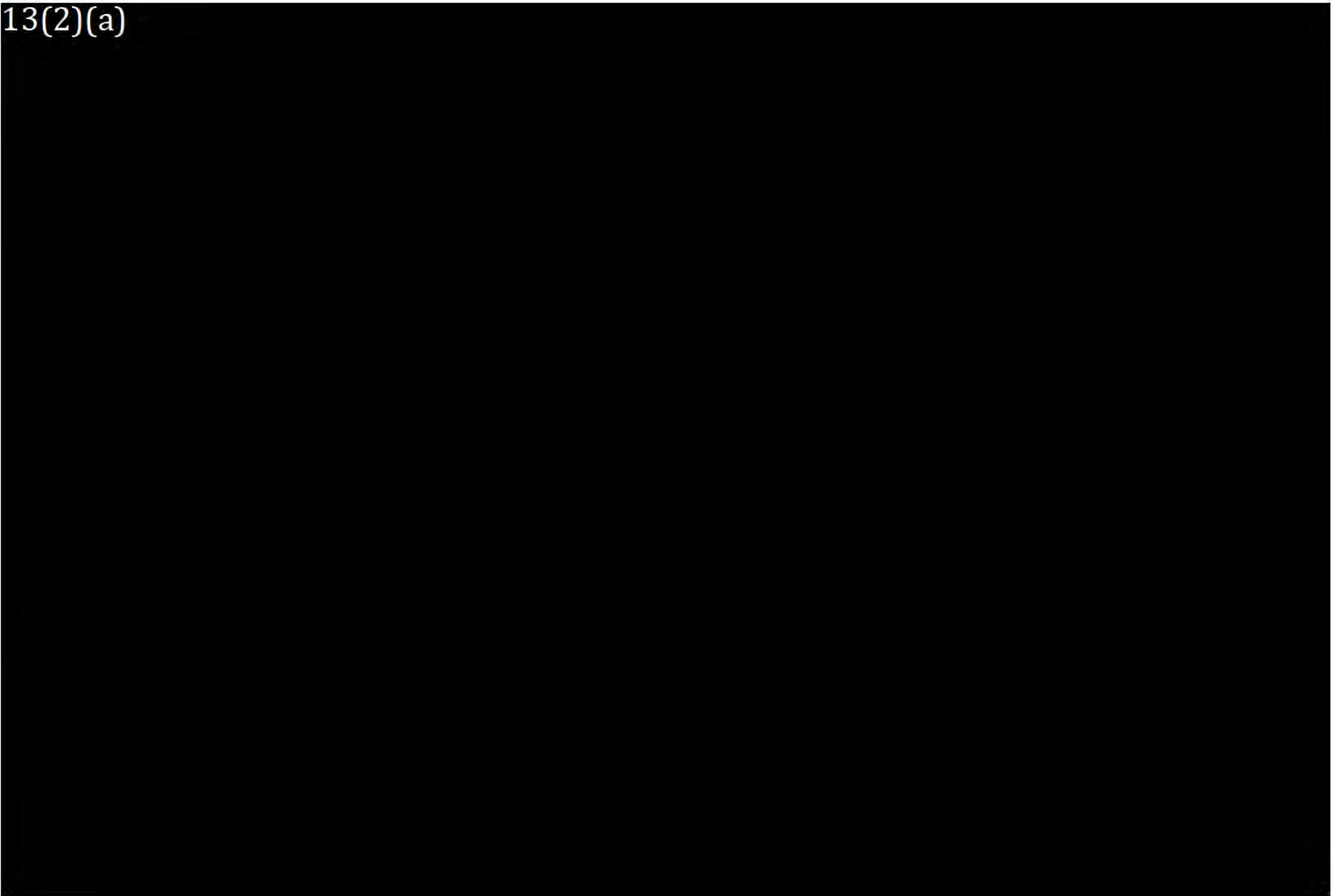
13(2)(a)



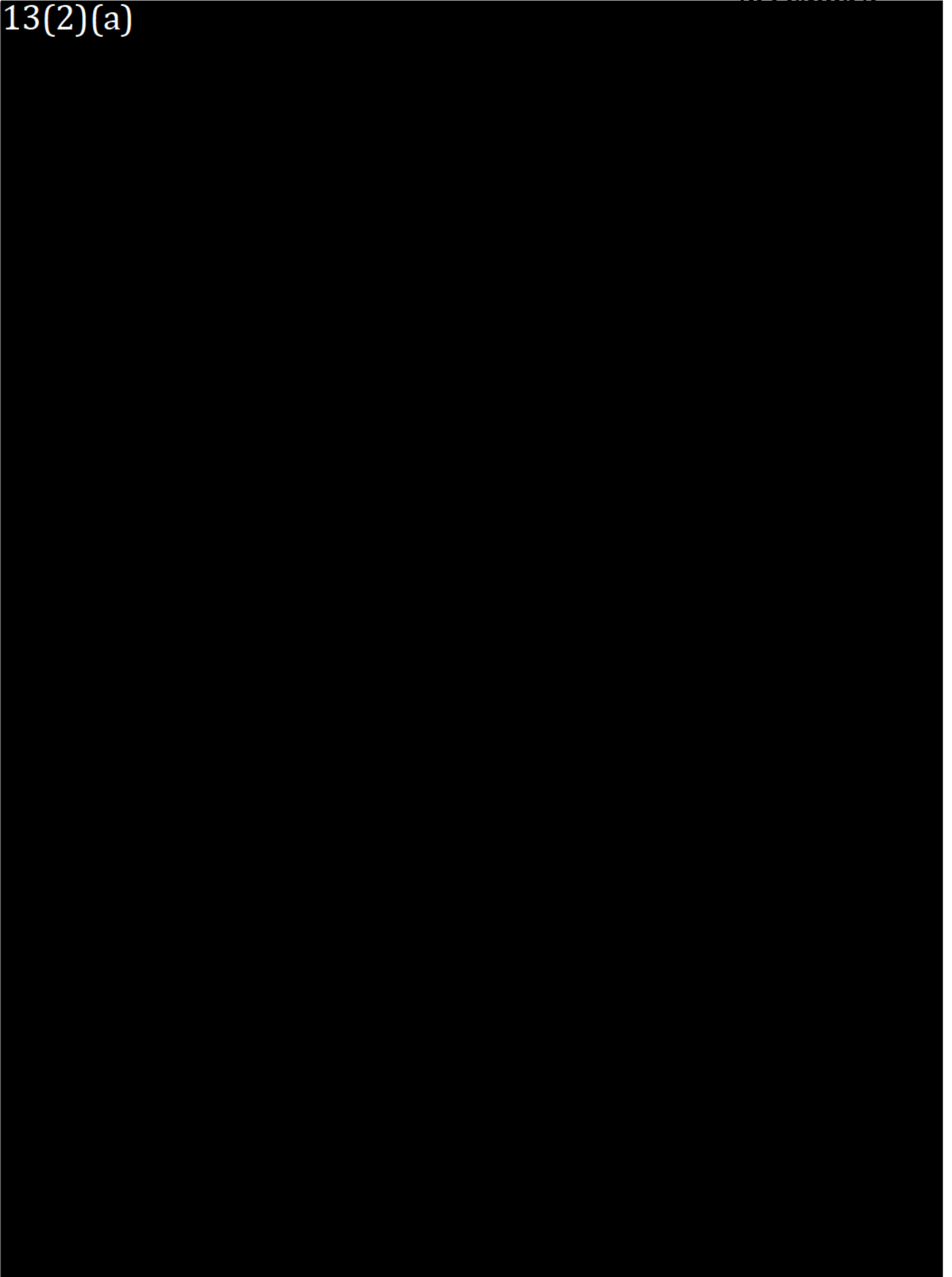
13(2)(a)



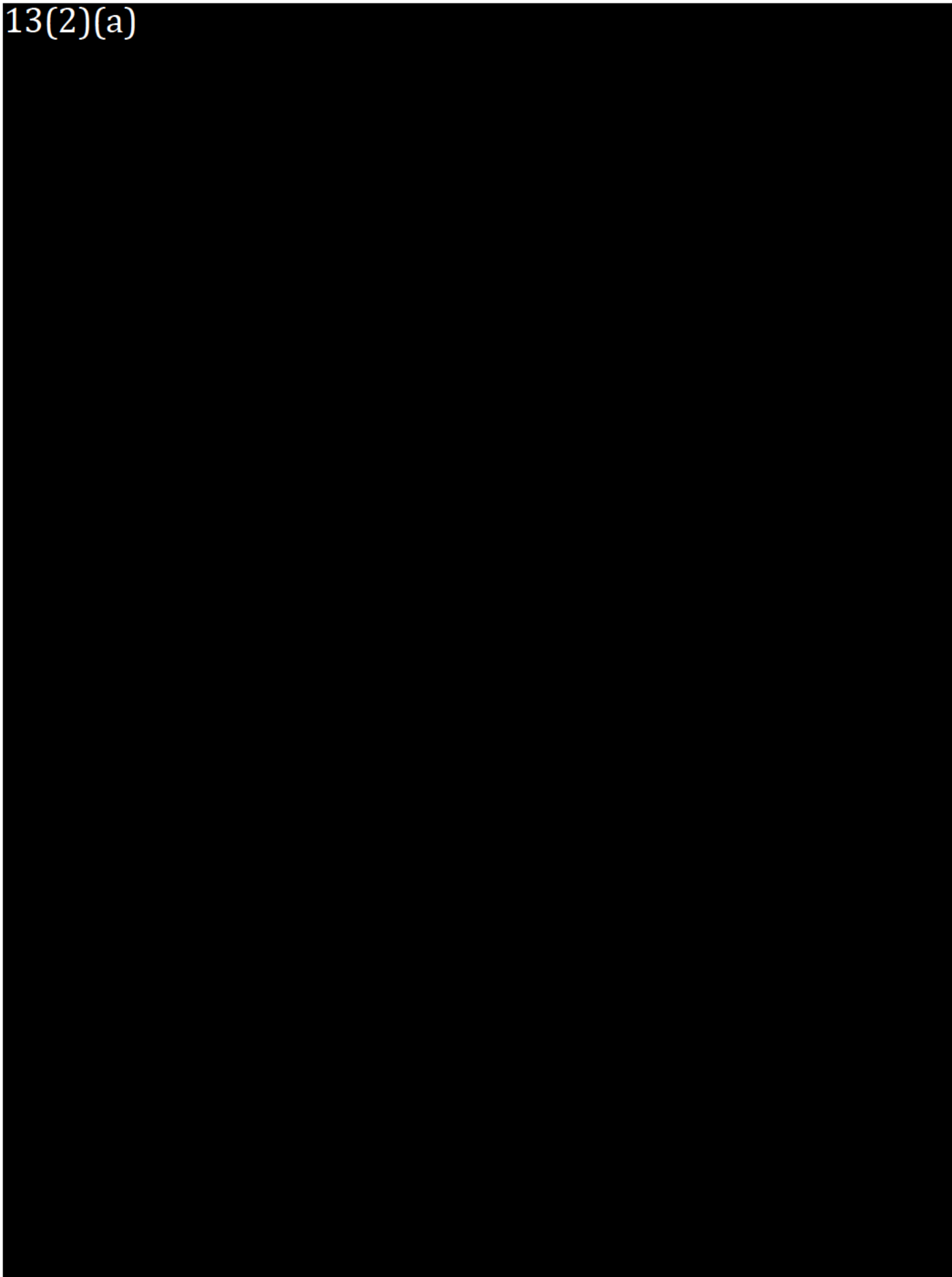
13(2)(a)



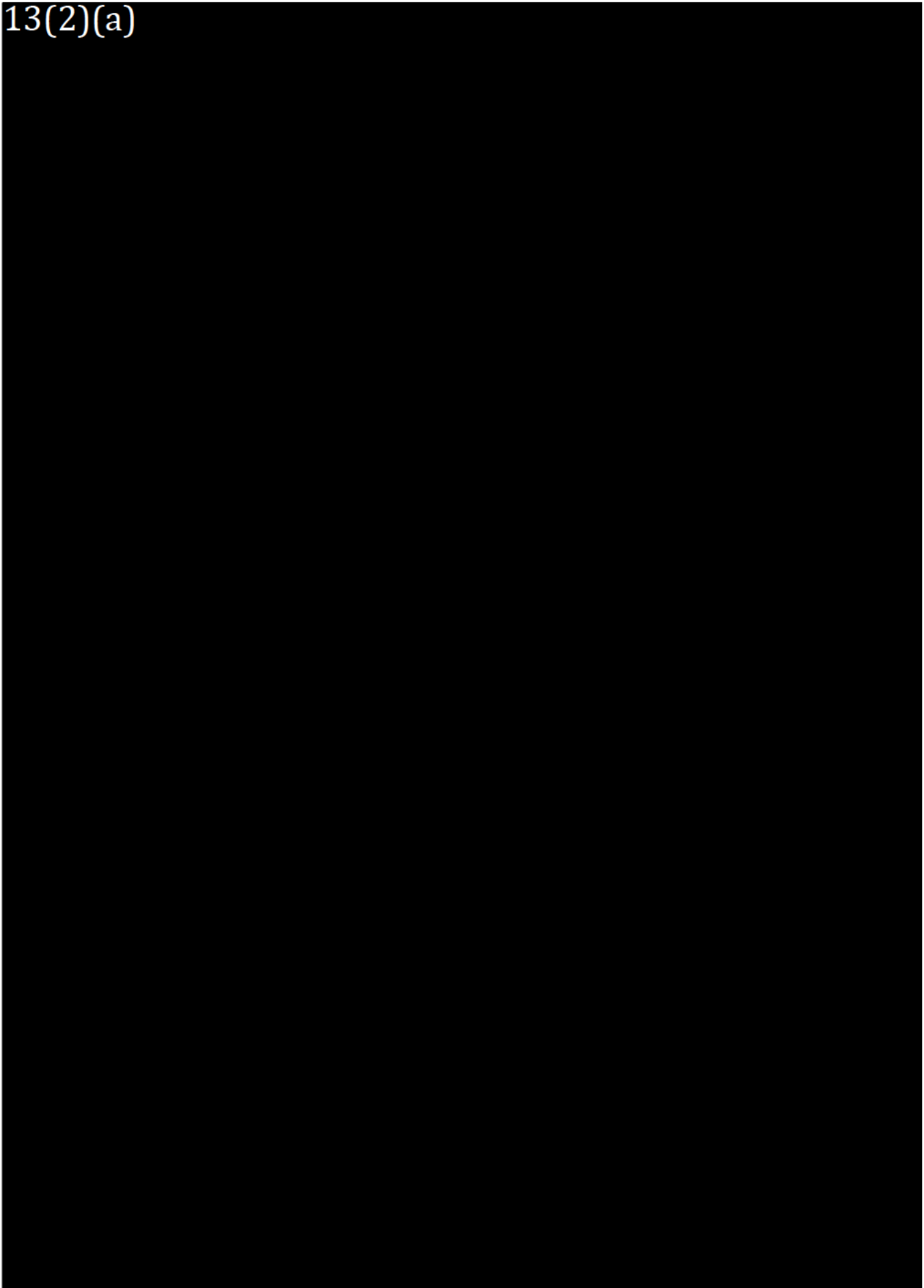
13(2)(a)



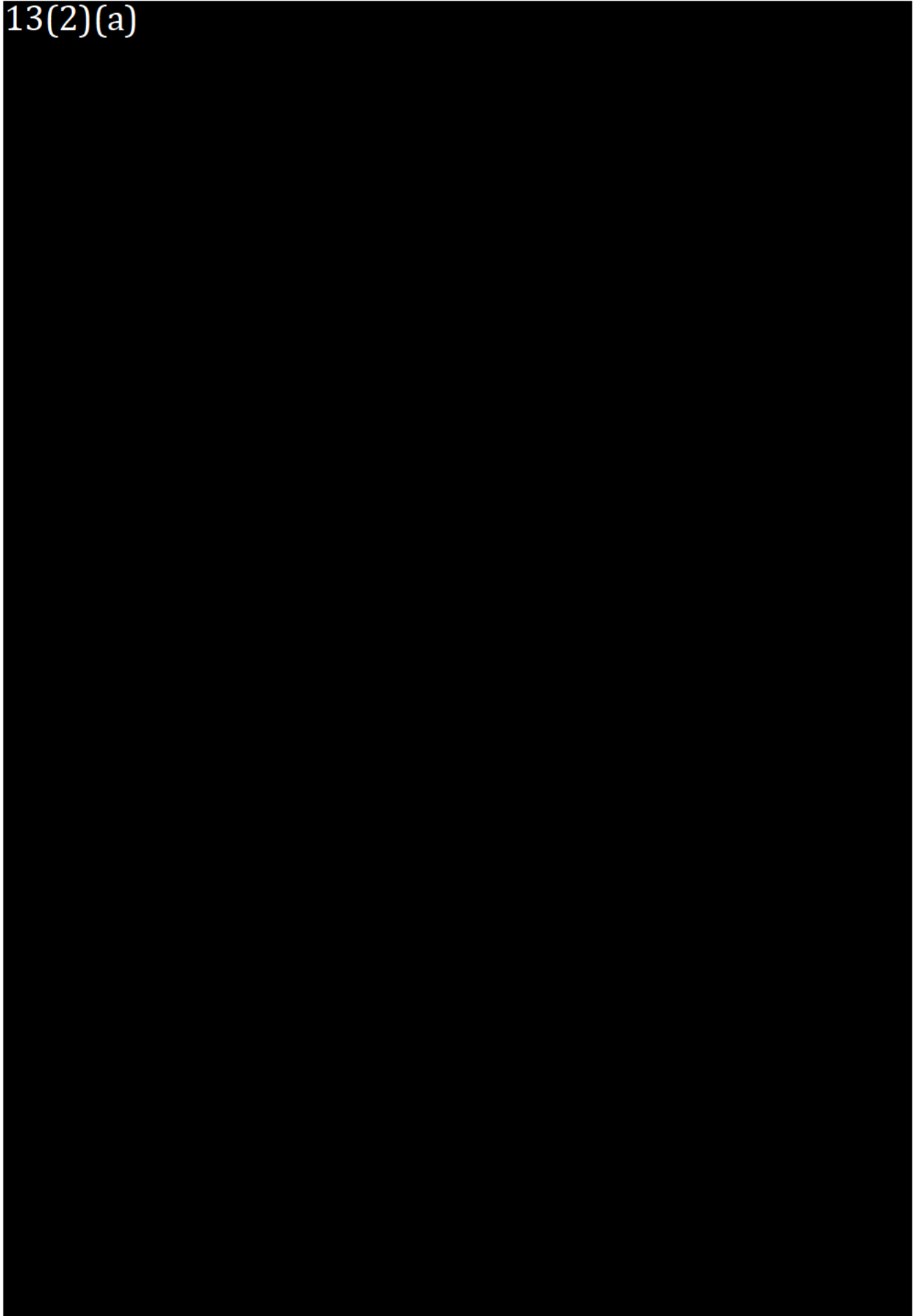
13(2)(a)



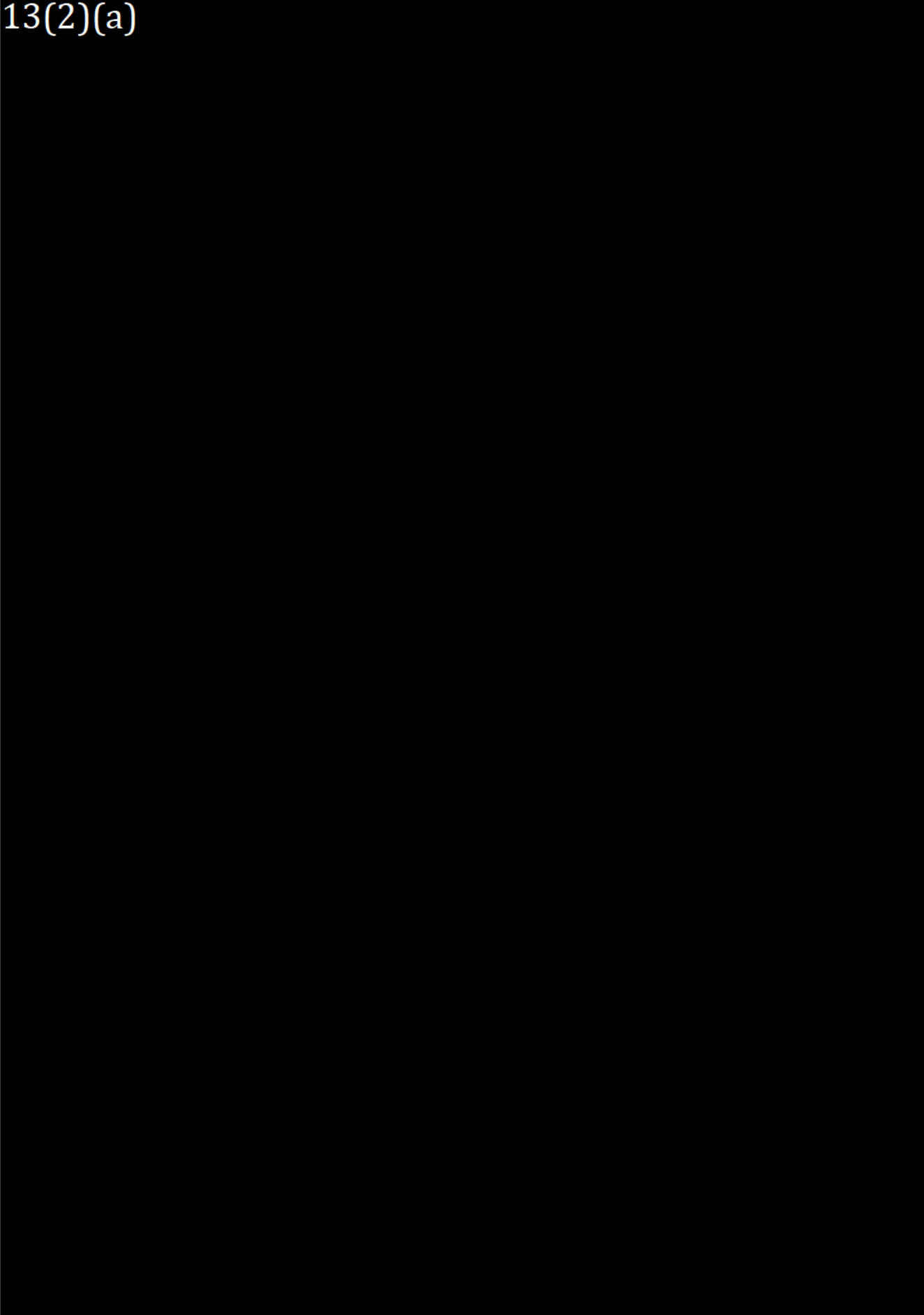
13(2)(a)



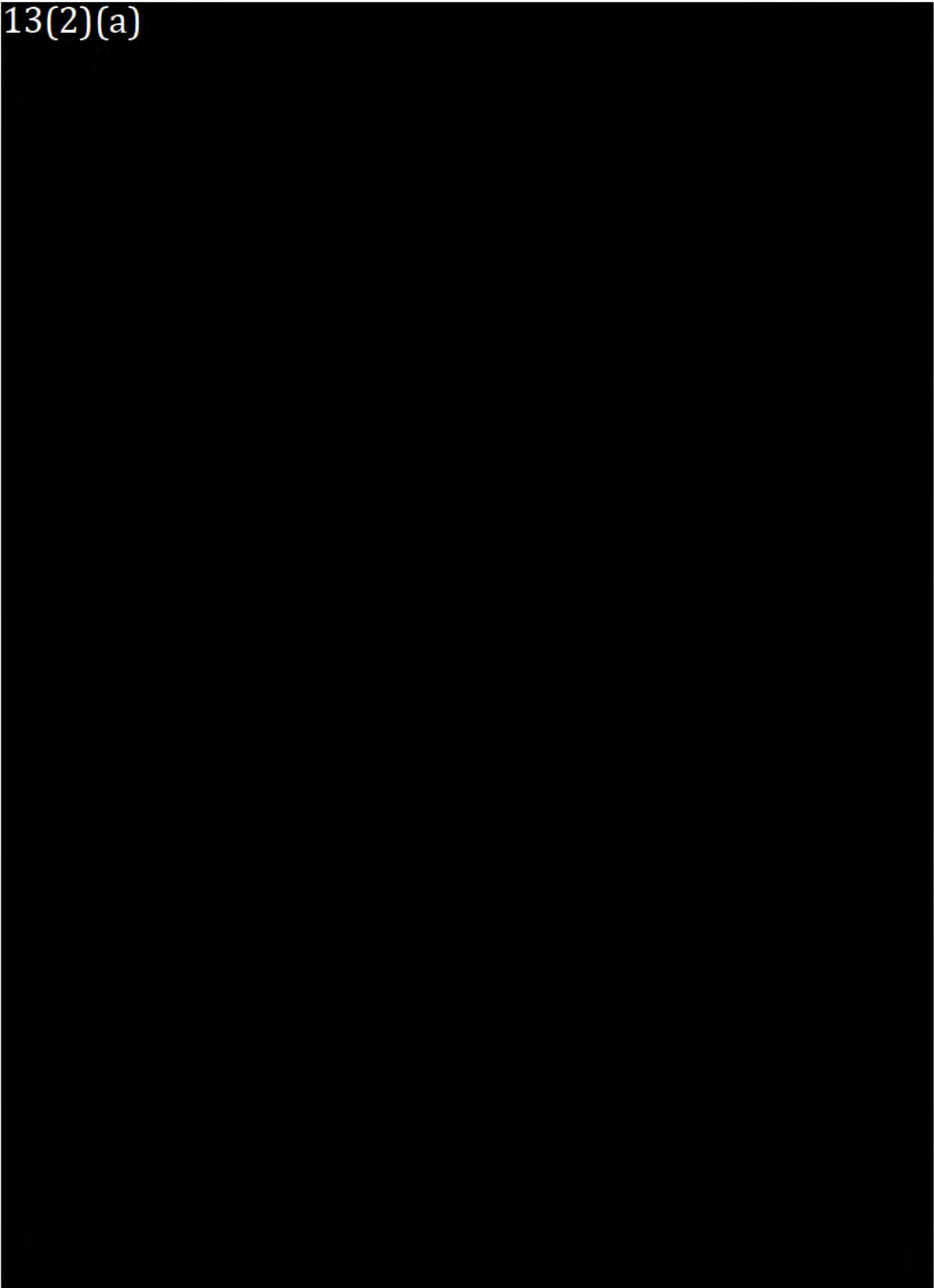
13(2)(a)



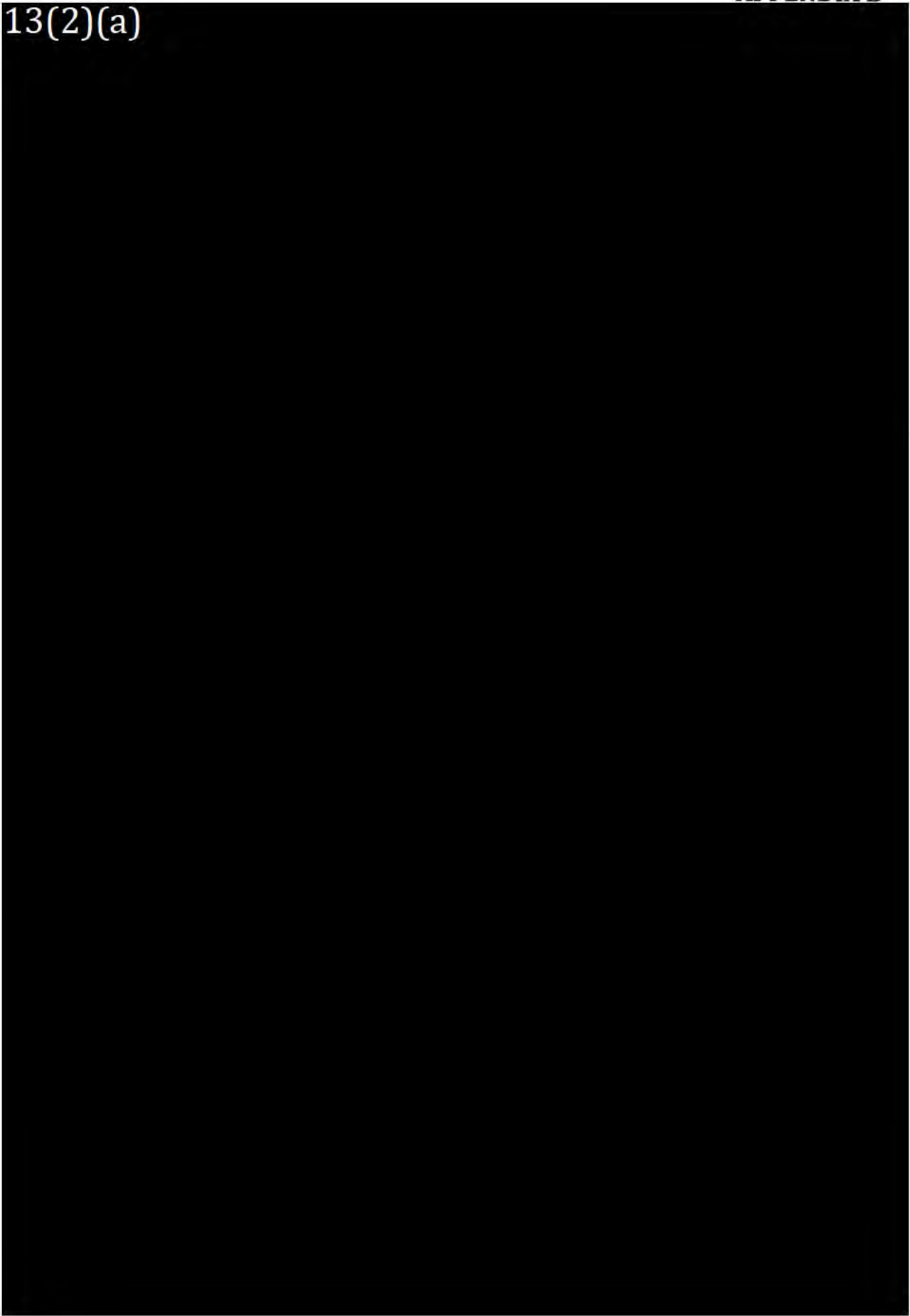
13(2)(a)



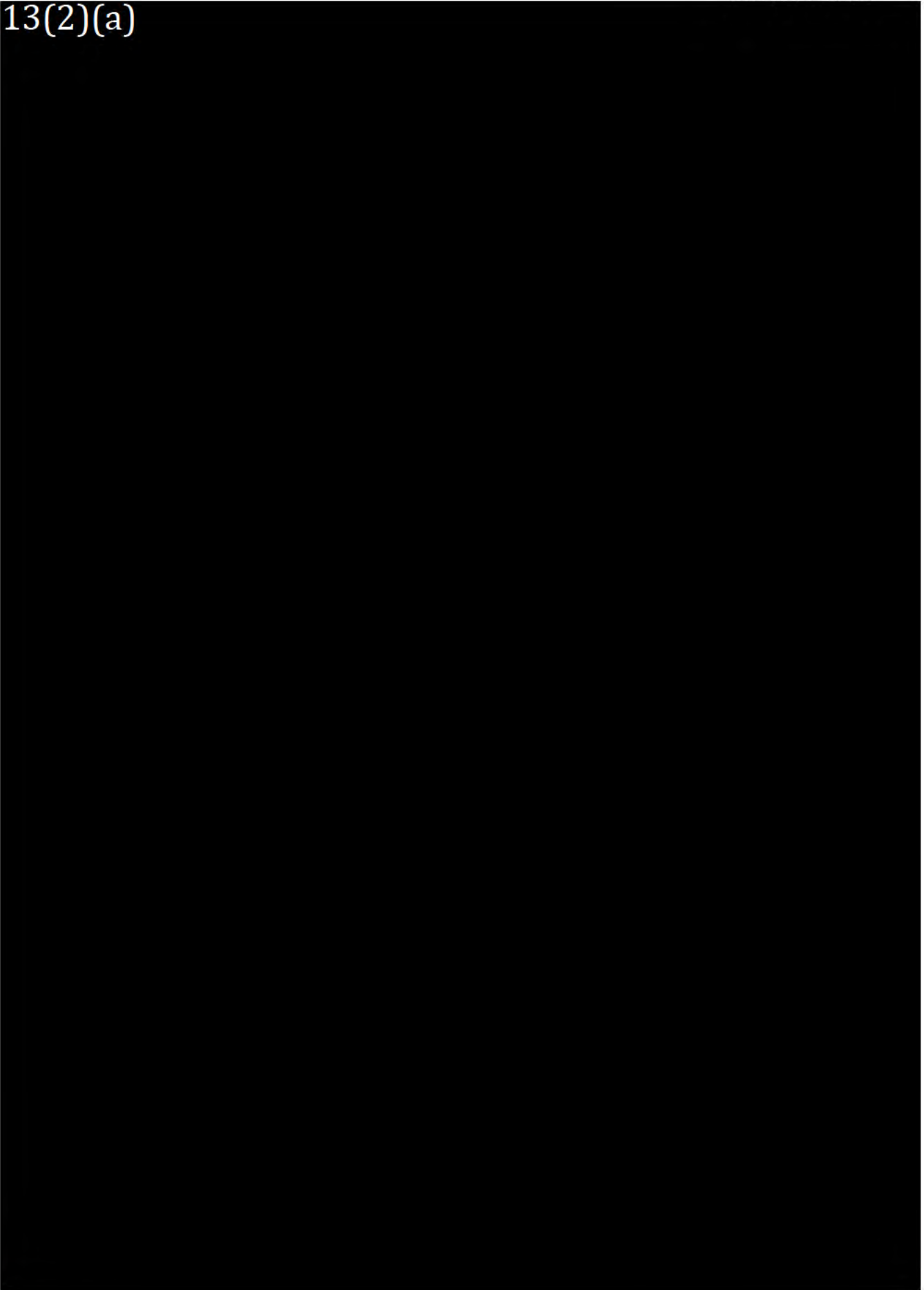
13(2)(a)



13(2)(a)



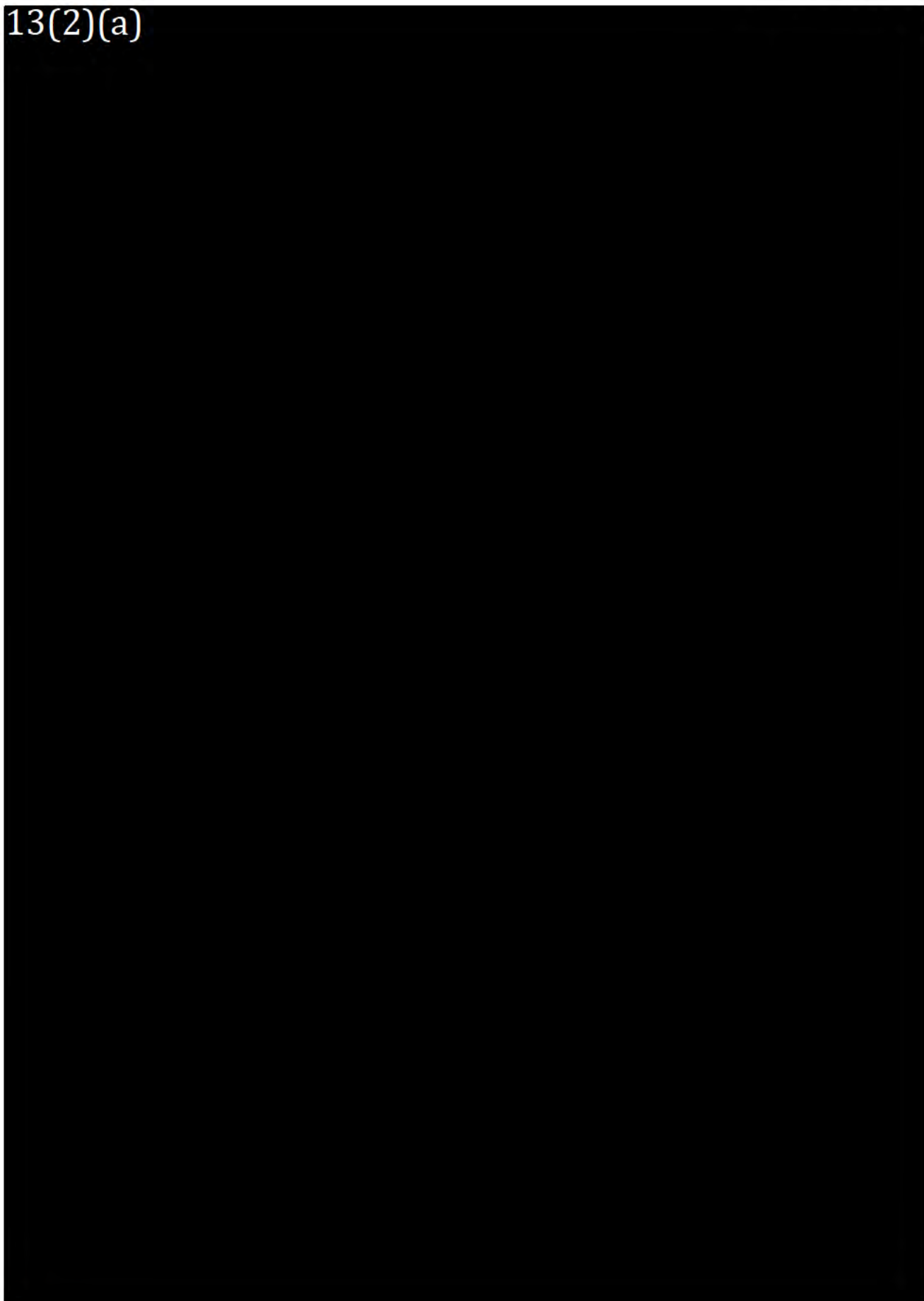
13(2)(a)



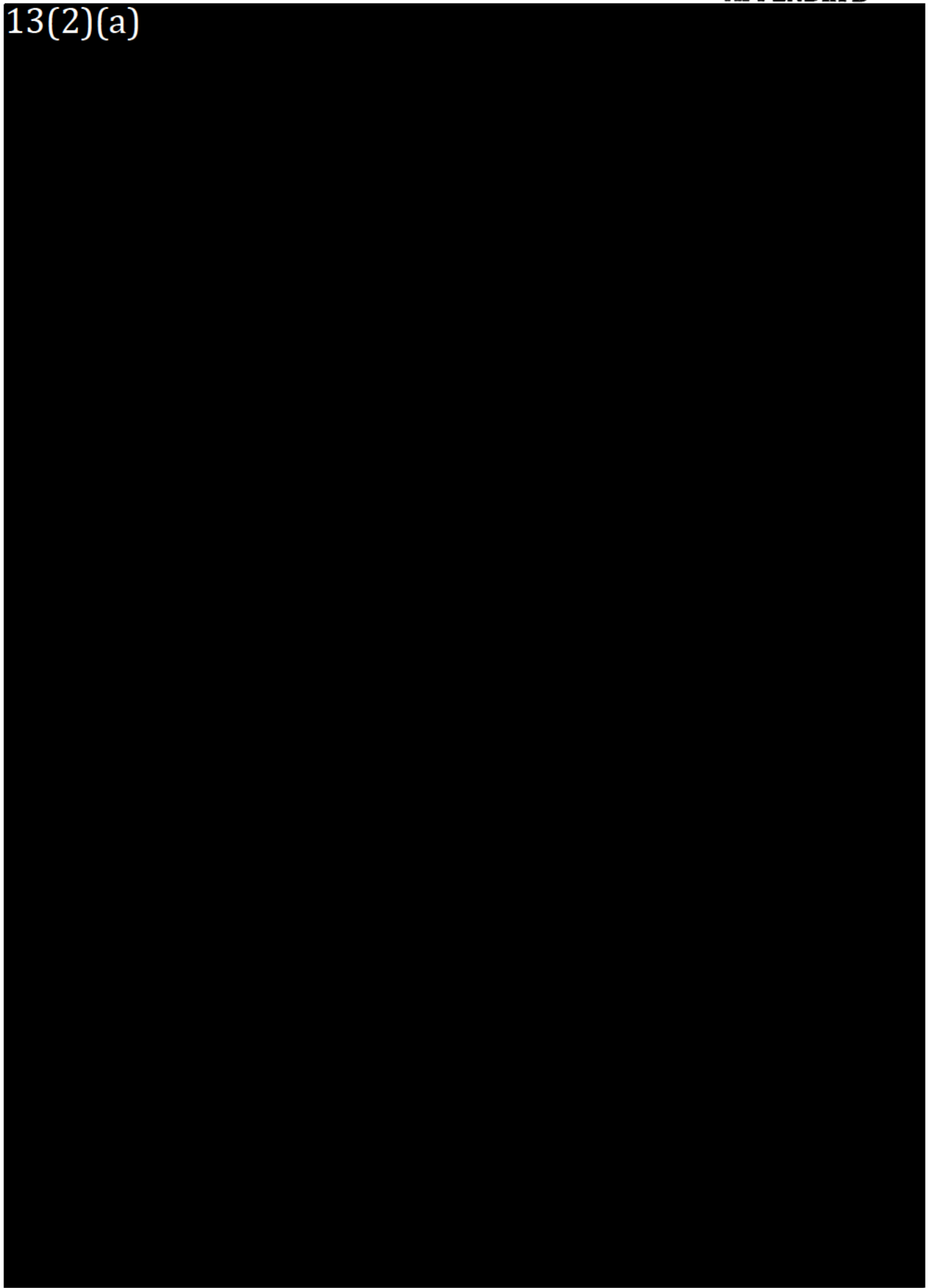
13(2)(a)



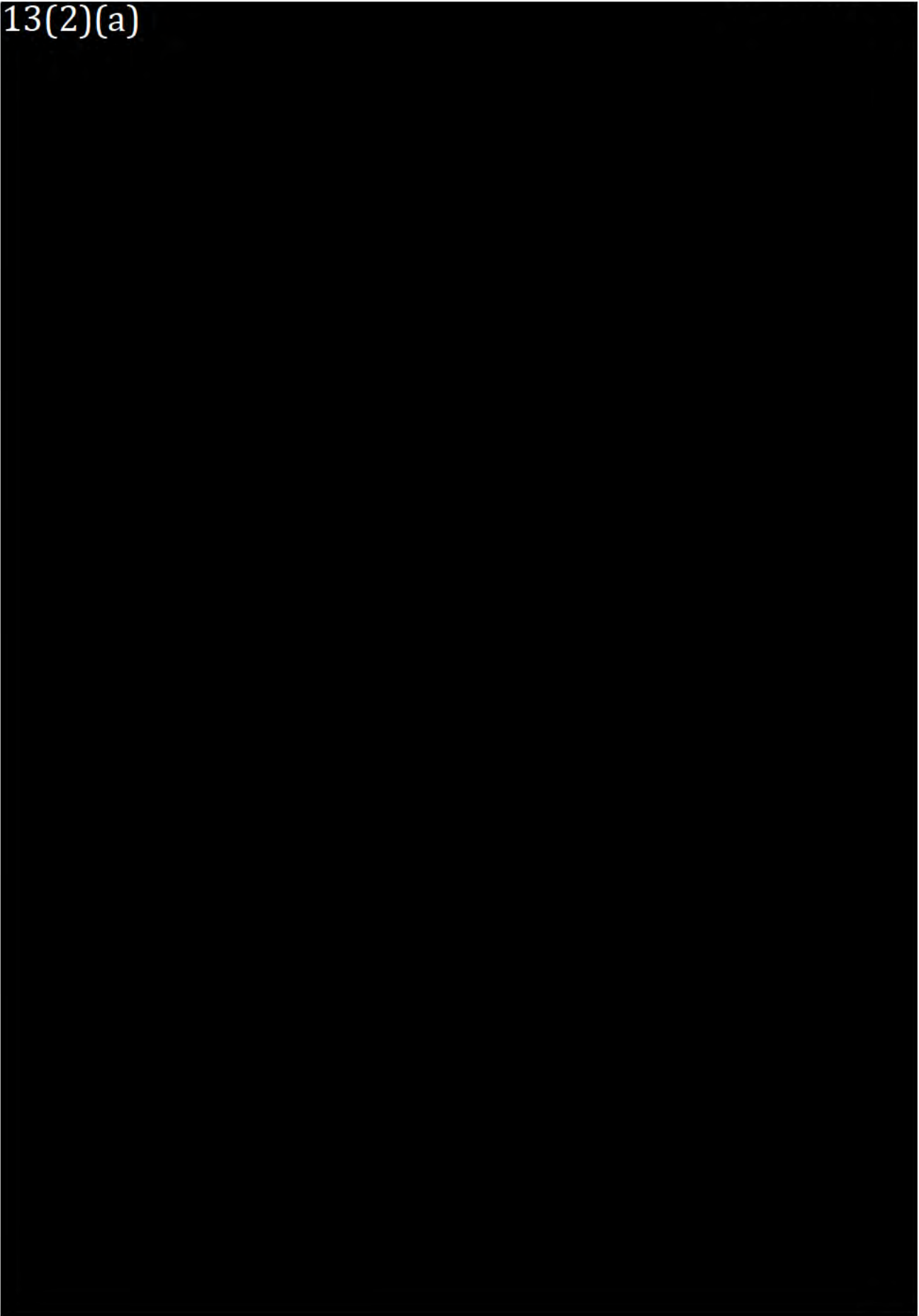
13(2)(a)



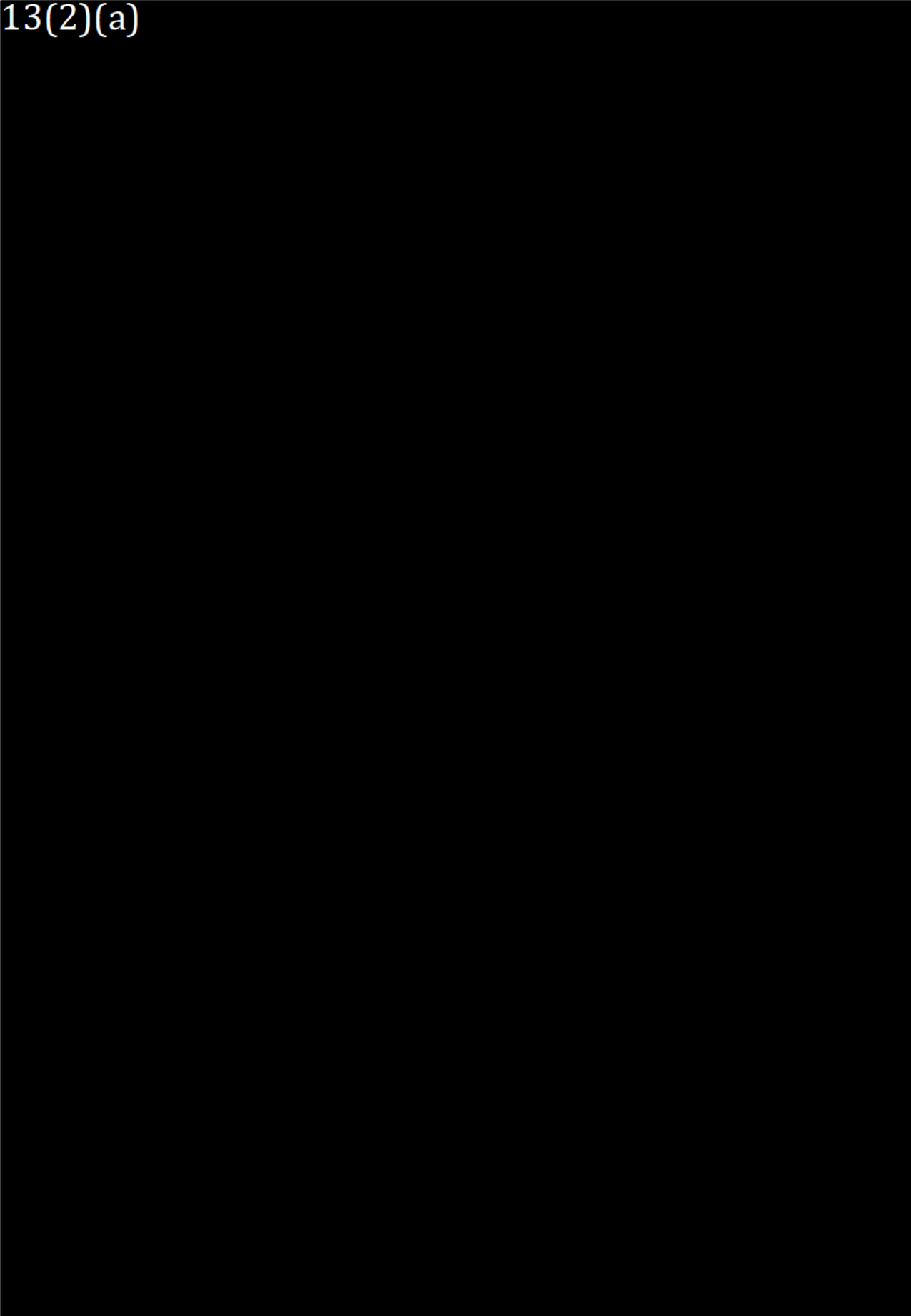
13(2)(a)



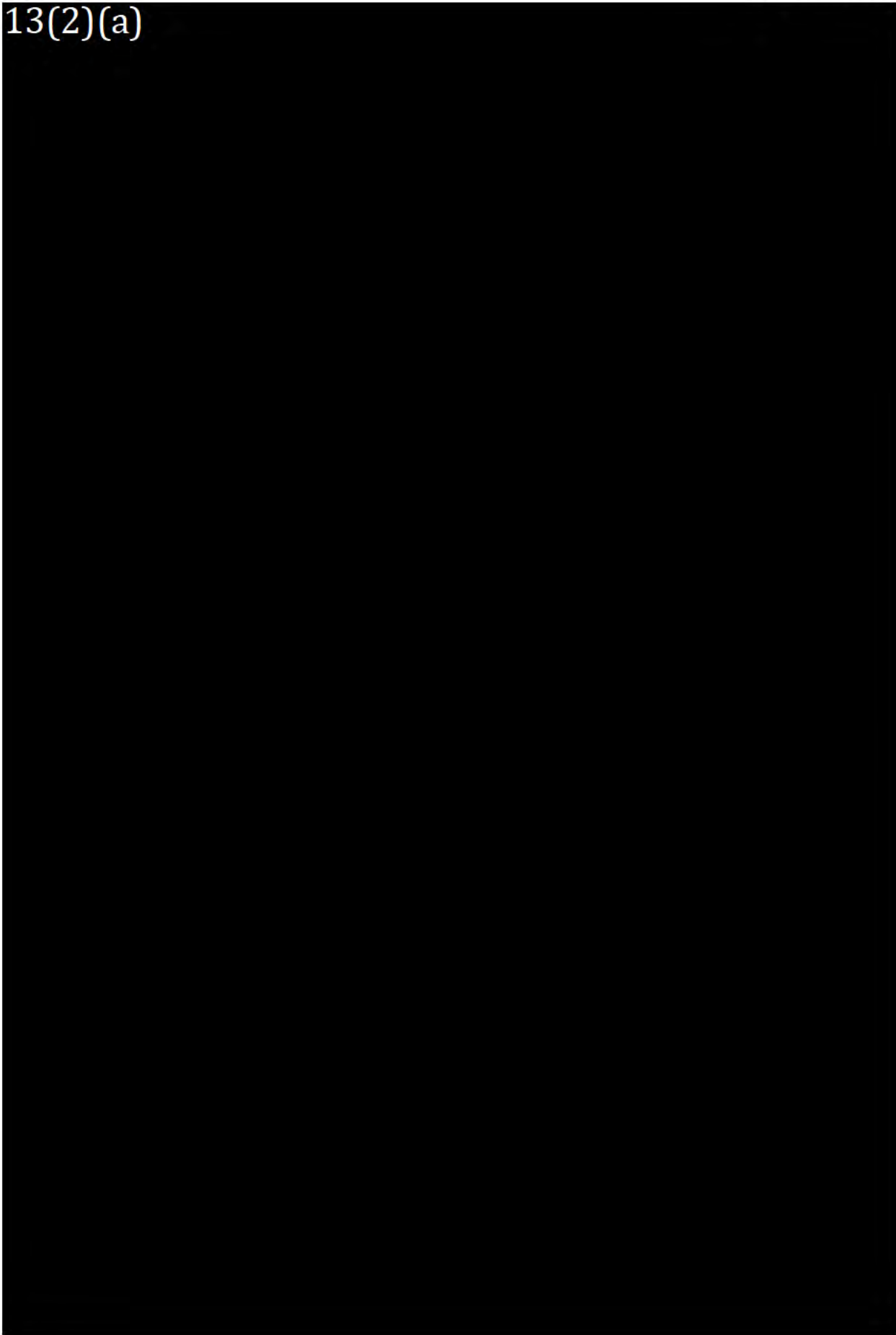
13(2)(a)



13(2)(a)

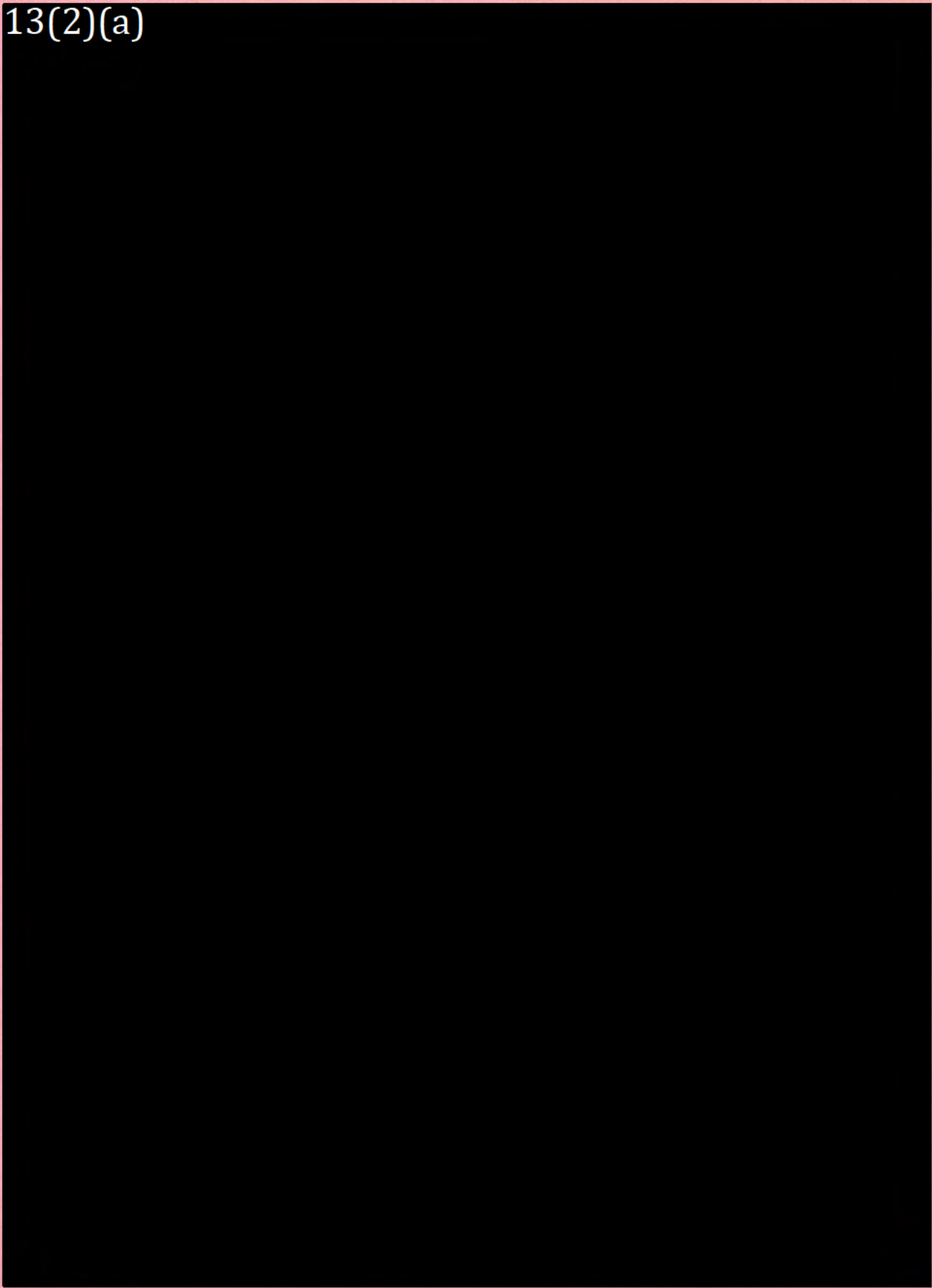


13(2)(a)

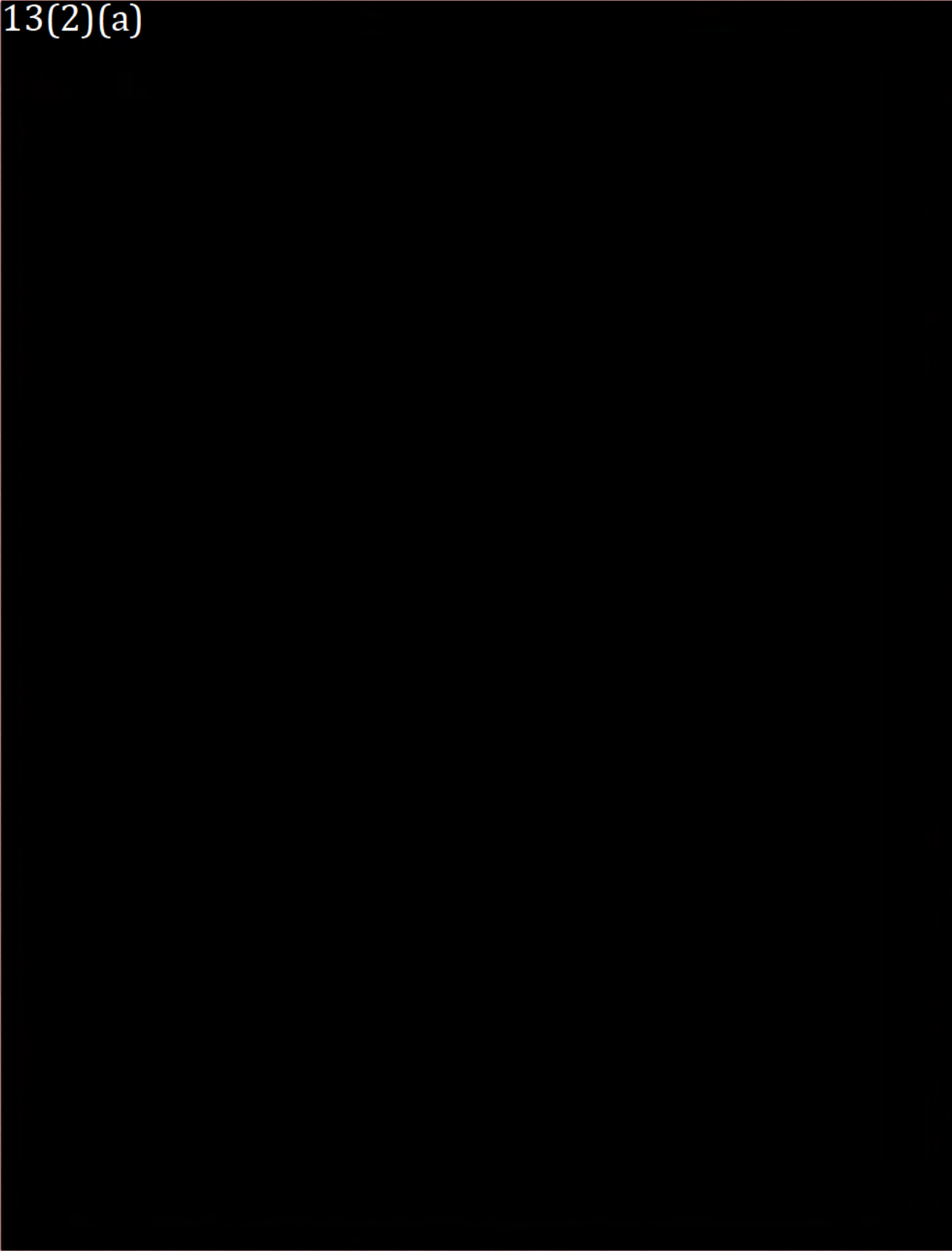


CONFIDENTIAL

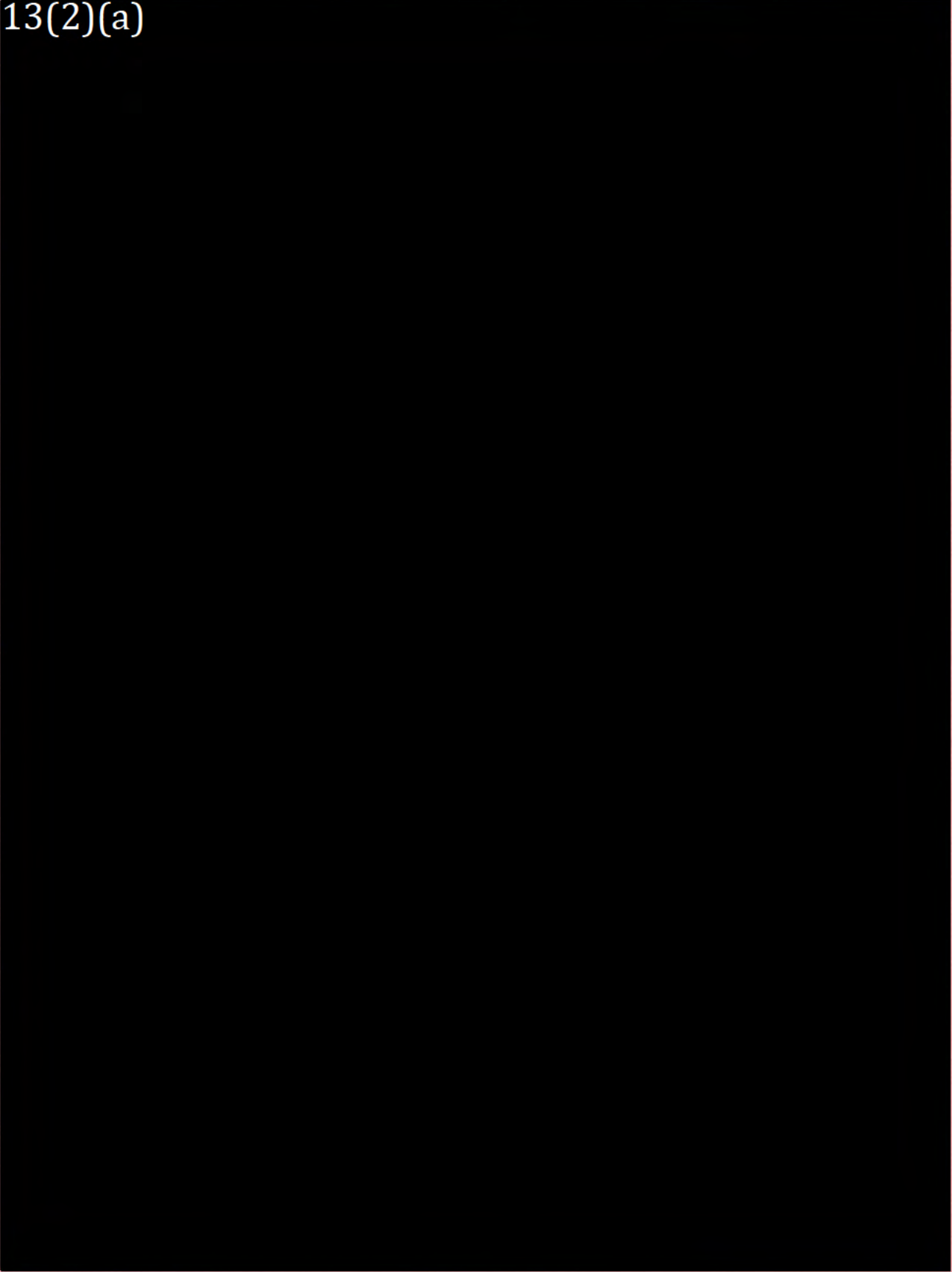
13(2)(a)



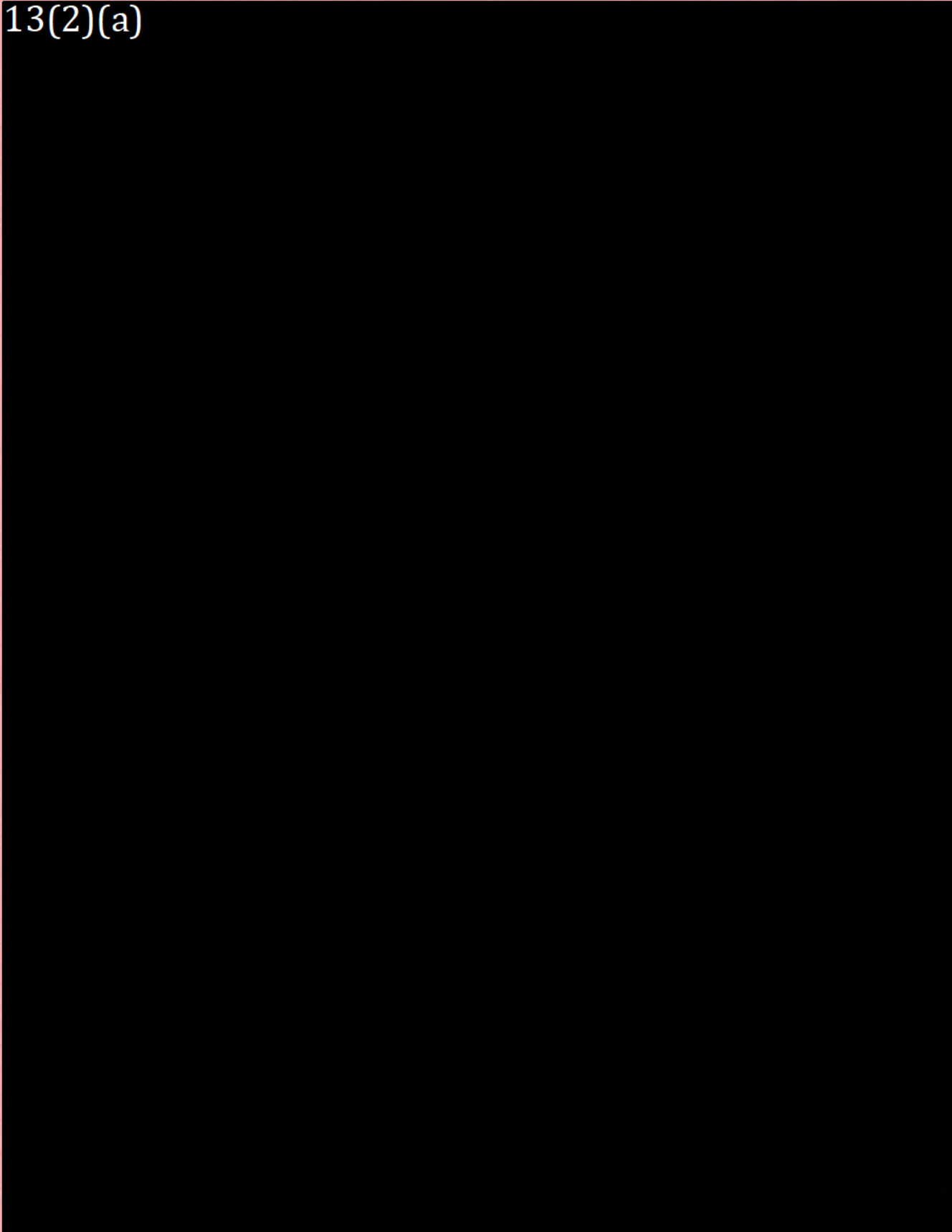
13(2)(a)



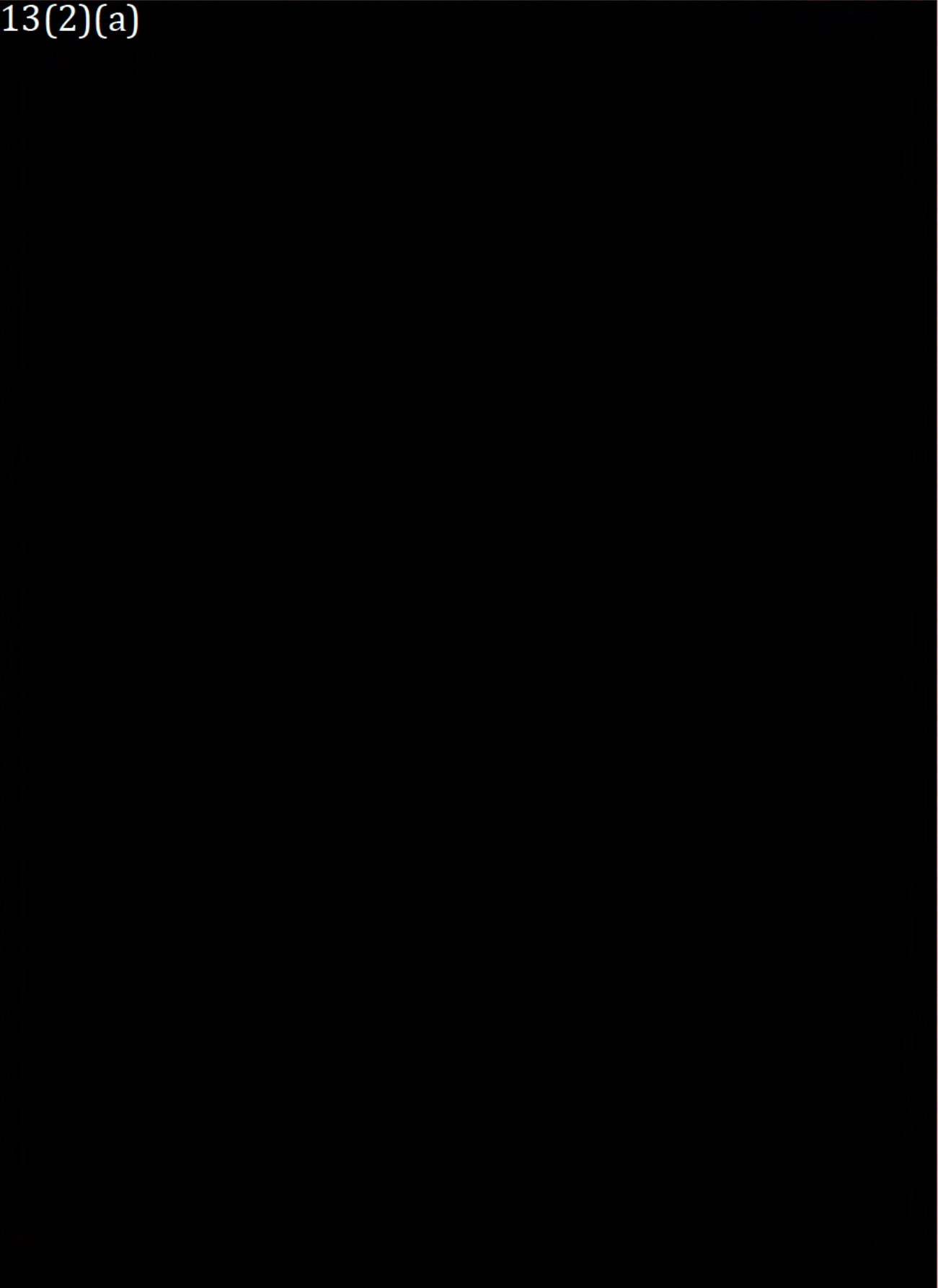
13(2)(a)



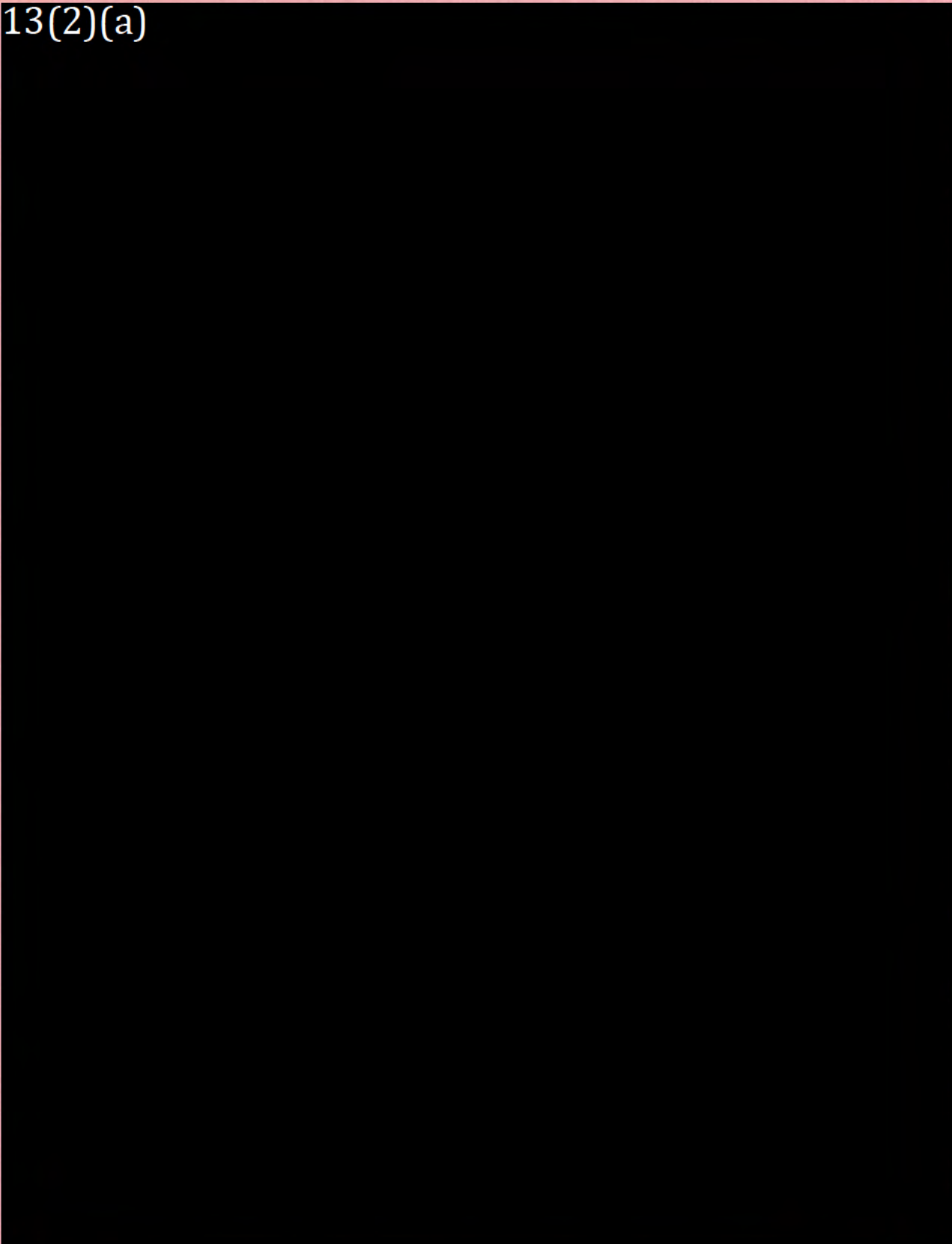
13(2)(a)



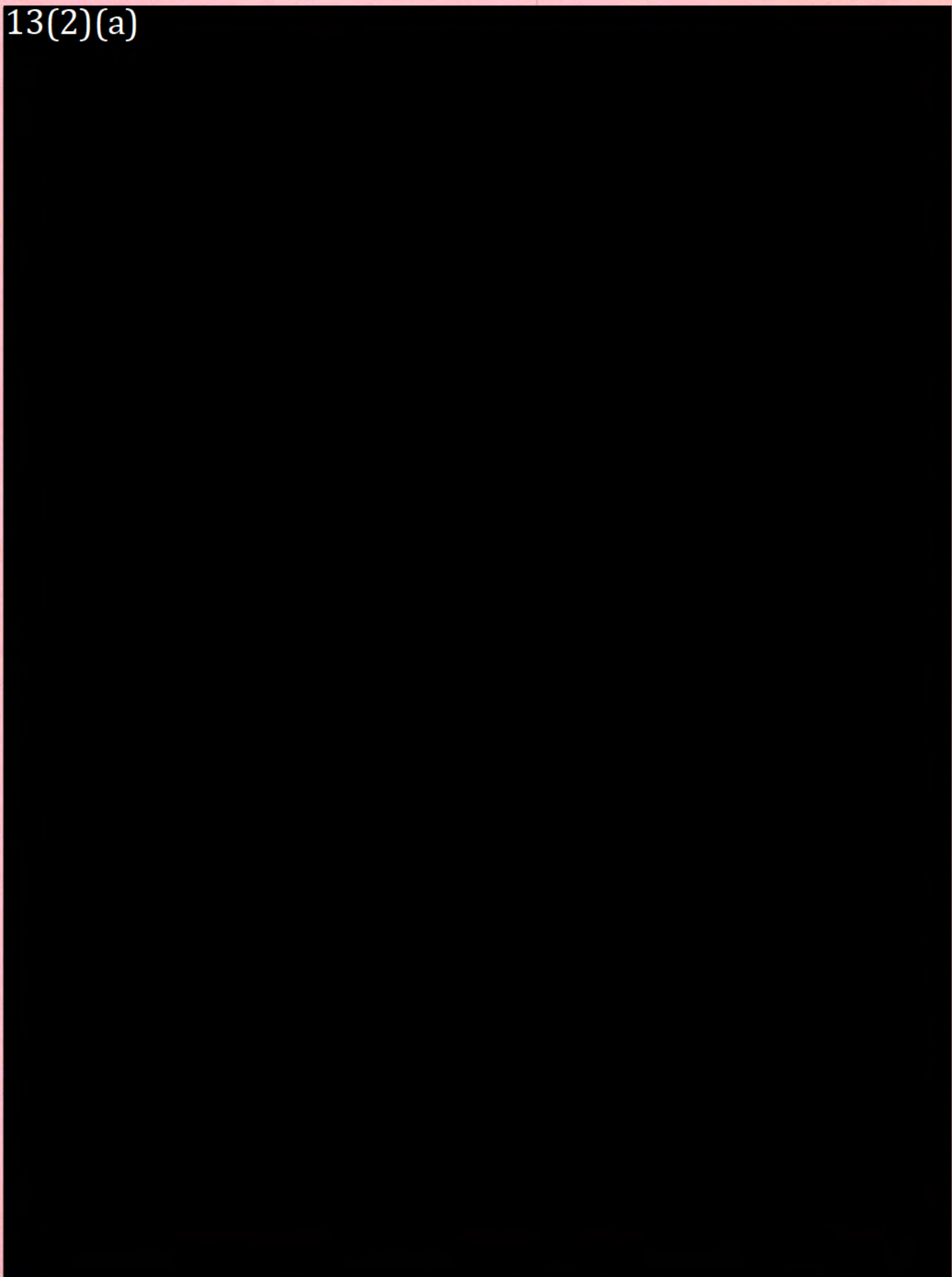
13(2)(a)



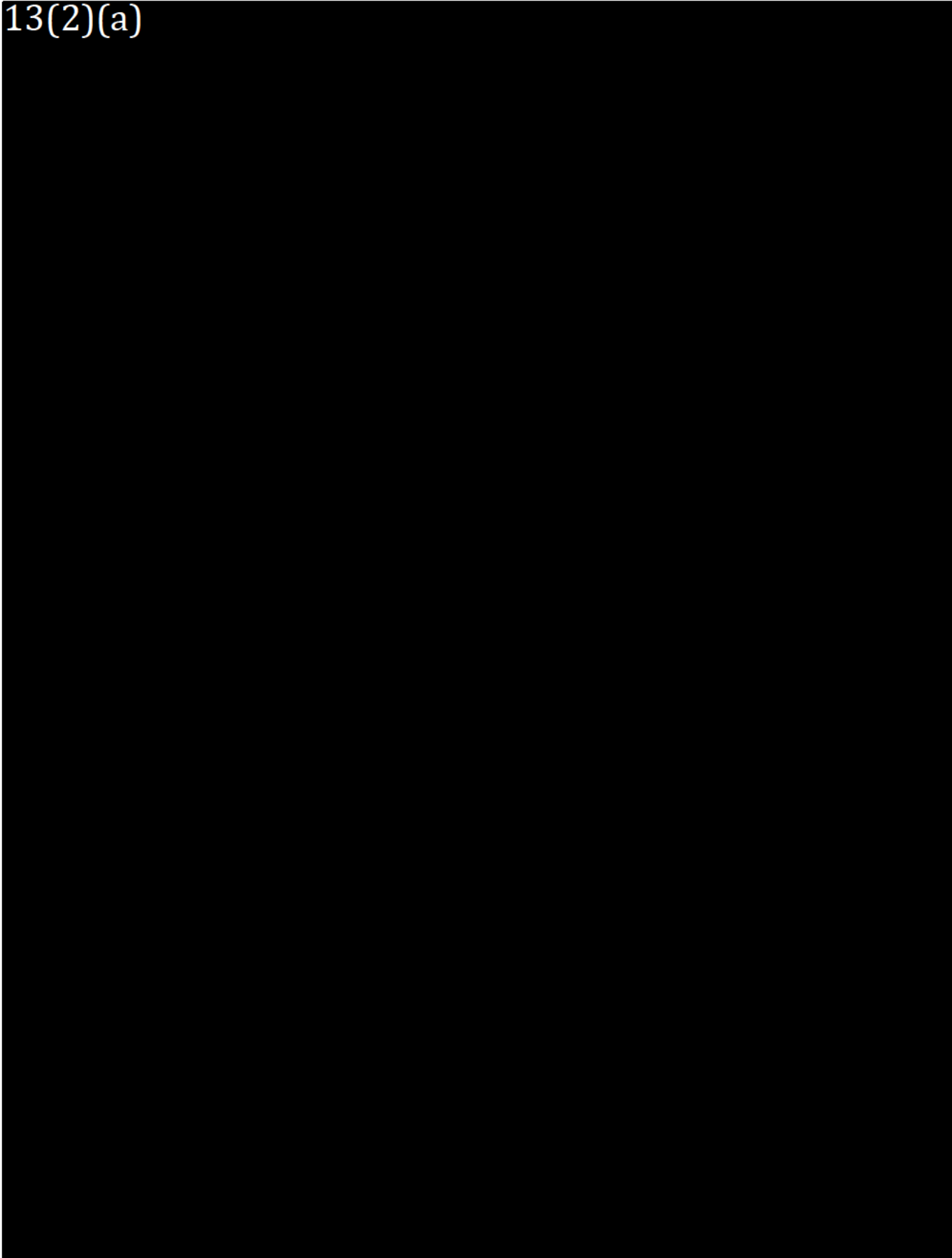
13(2)(a)



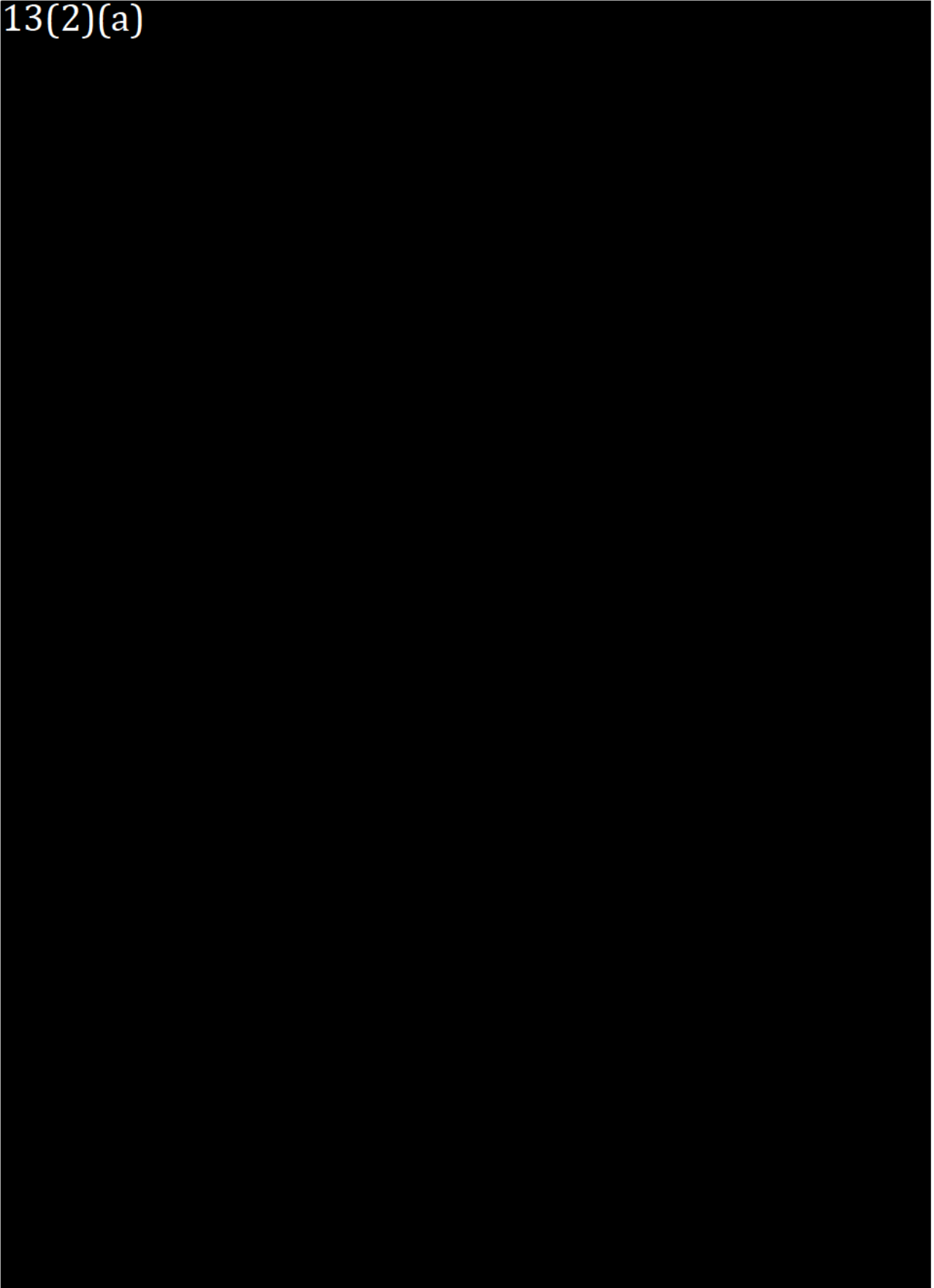
13(2)(a)



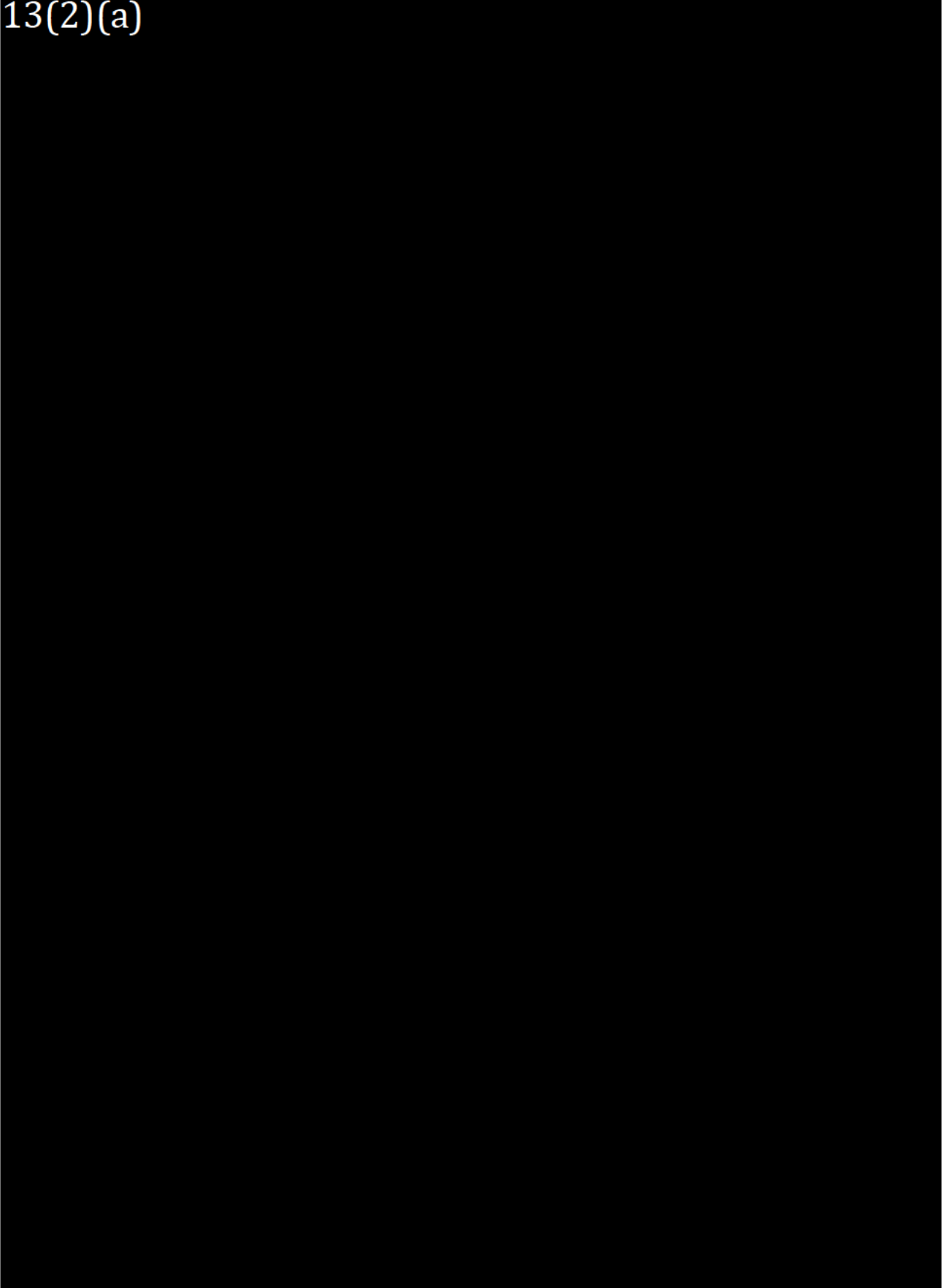
13(2)(a)



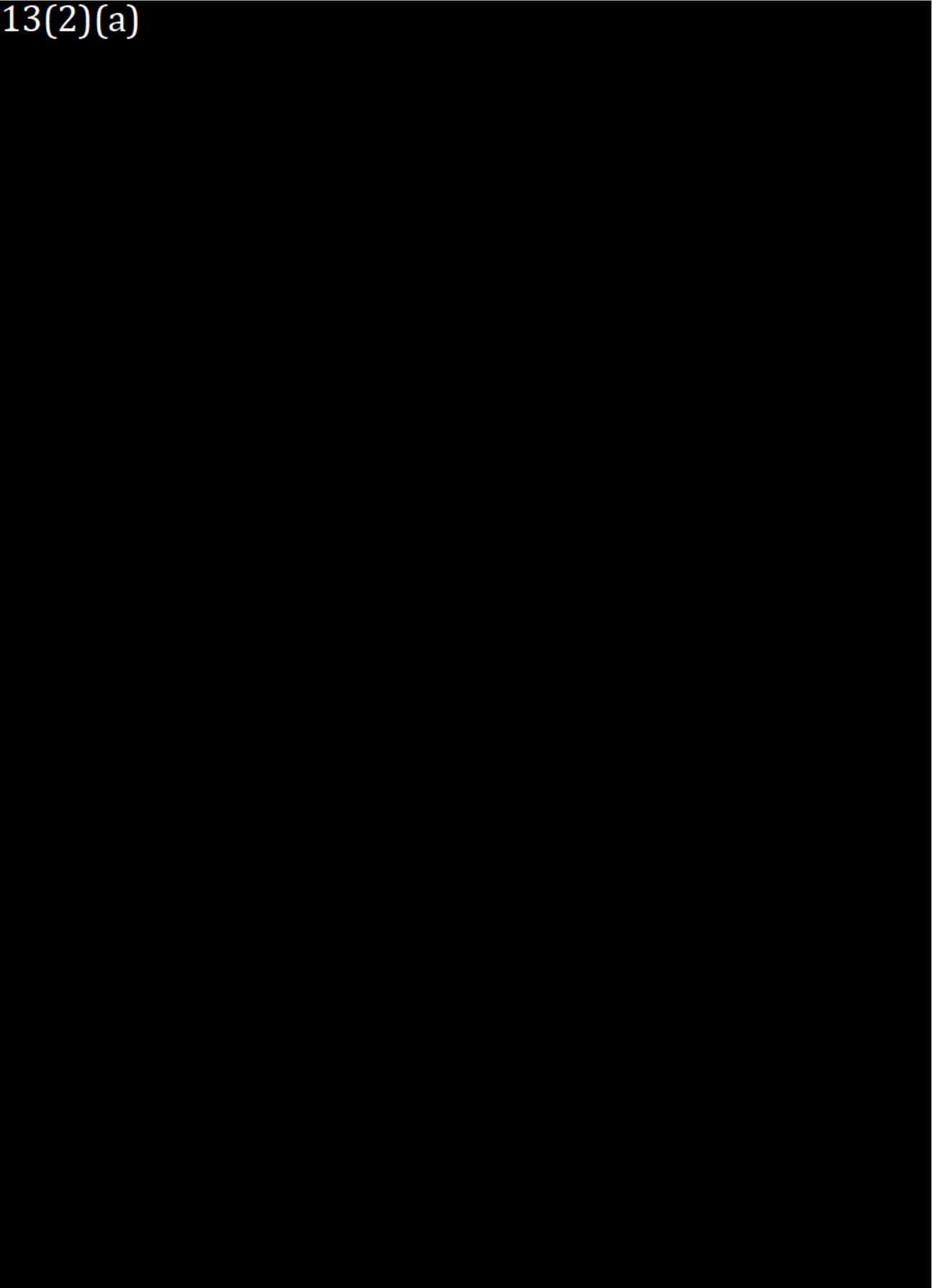
13(2)(a)



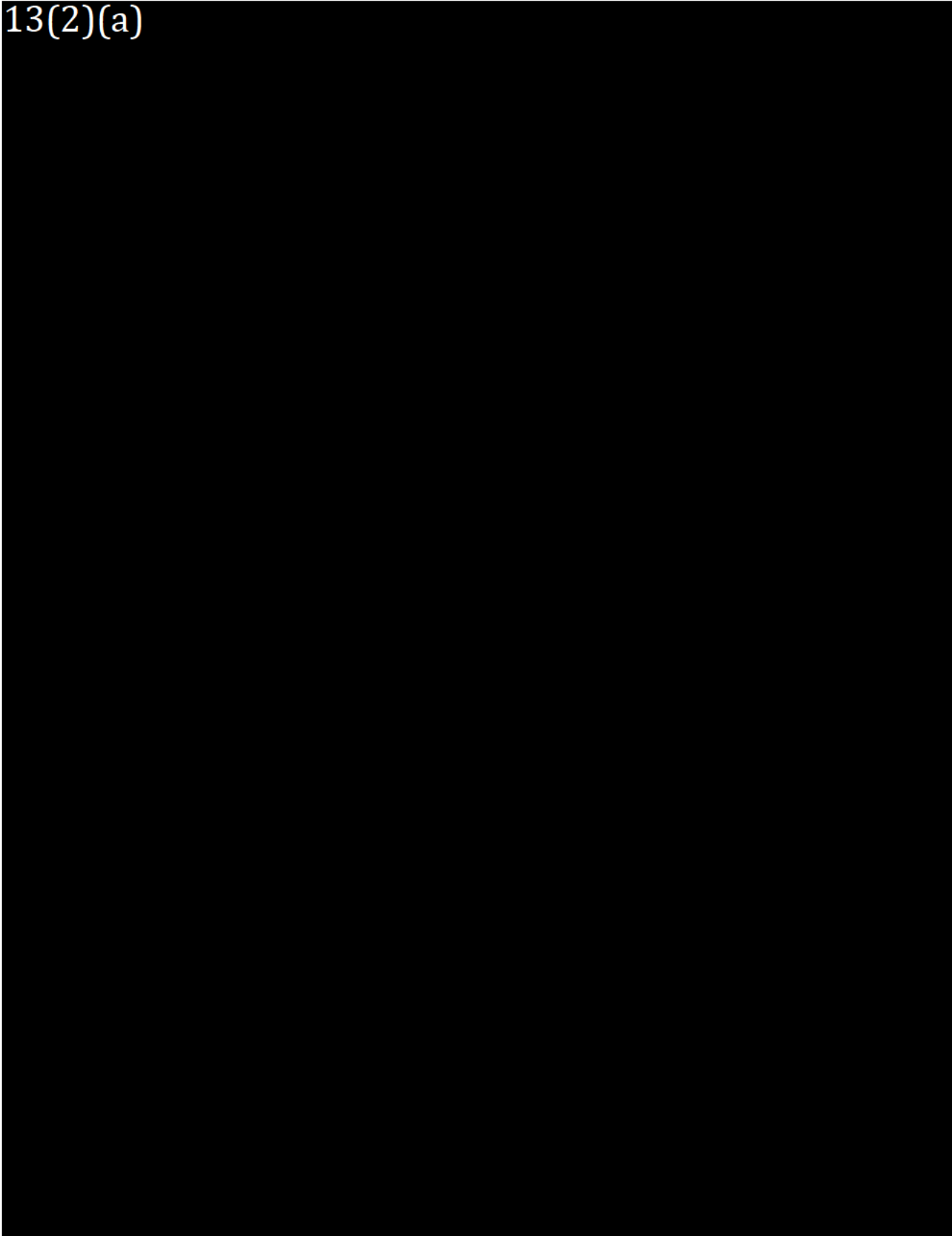
13(2)(a)



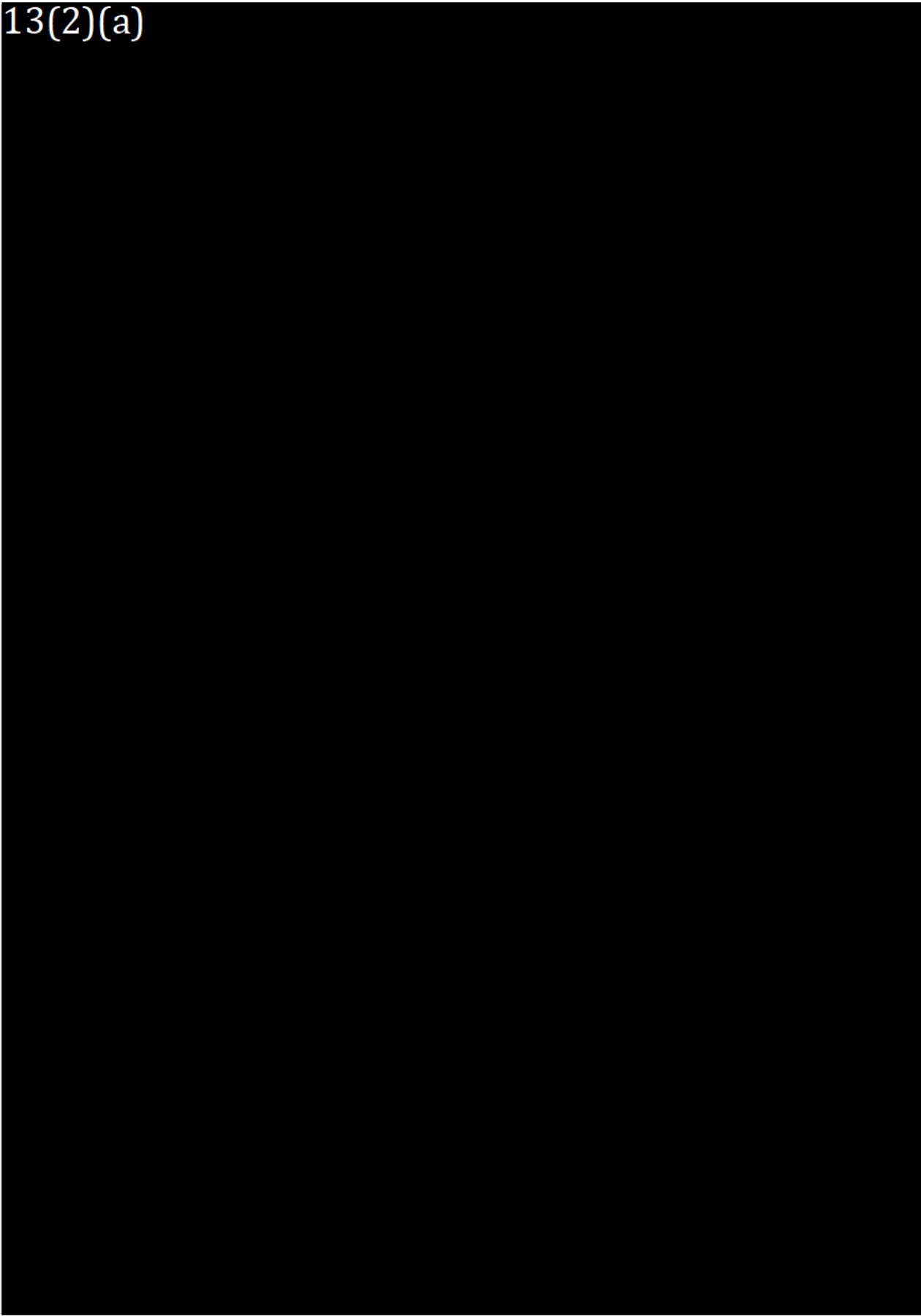
13(2)(a)



13(2)(a)



13(2)(a)





JUN 29 2018

CONFIDENTIAL

File: 7820-20-LND-151-102

MR. WILLARD HAGEN
DEPUTY MINISTER
LANDS

Management Letter: Commissioners Land Lease Assessment
Review Period: August 1, 2017 to May 31, 2018

Scope and Objective

The Audit Committee approved the management requested consulting service for the Lands Administration Division (Division) in the Department of Lands (Department). The project objective was to conduct an independent quality assessment of the Division's documented processes to assess if the internal controls were adequate to ensure the change in the Commissioner's land lease process was in compliance with the Northwest Territories *Commissioner's Land Act*, *Commissioner's Land Regulations* (Regulations).

The project scope was the Commissioner's land lease application process (lease process) in three NWT regional offices. The Division implemented the change in lease process during the review period; the integrity of data was not tested due to the inadequate sample size of transactions.

Transfer of Land Process Responsibility

Prior to April 1, 2014, the Department of Municipal and Community Affairs was responsible for administering the Regulations. Administration of Commissioner's Land was carried out in the regional offices. On April 1, 2014, the administration of the Regulations was transferred to the Department.

This document may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.

The GNWT created and placed the Commissioner's Land and Territorial Land processes in the Division. The purpose was to ensure consistency in processing land transactions in the NWT. The Division staff created written procedures, conducted on site training and distributed process flowcharts to ensure the land process changes were understood during implementation.

Audit Examination

During the review period Internal Audit Bureau (IAB):

- reviewed the Regulations, procedures and documents on the land application process used by the regions
- mapped the lease process and compared it with the original flowchart prepared by the Division (**Schedule 1, Appendix A refers**)
- interviewed the regional staff to verify the lease process steps followed as of February 2018.

Communication to Management

On June 7, 2018, IAB staff met with the Division's Director and the Department's Director of Finance and Administration to communicate the results of the assessment (**Schedule 1 refers**).

Findings and areas to consider

1. Inconsistencies with the implementation of the planned changes were found in the following areas:
 - a. Completing lease applications
 - b. Execution of signed lease agreements
 - c. Dissemination of lease process reference material.

2. Management discussion of inconsistencies:
 - a. Receipt and completion of land applications will be completed by clients in the regions. Regional staff may provide assistance to clients on completing the applications but may not fill in the applications for them. The lease approval and data entry will be conducted in the Division. The lease process will be clarified internally with Division and regional staff and then communicated to the public in a consistent manner.

- b. Administration of leases (and other legal instruments) was reorganized to be managed in the Division. This reorganization allowed the Division to facilitate the:
 - i. development of knowledge and skills to ensure the legal and financial obligations are met
 - ii. consistent processing of all lease agreements.

While the process requiring final execution of lease agreements was carried out by the Division, one Regional Superintendent continued to execute lease agreements in the region. According to regional staff, the rationale was to provide better customer service to the client.

The Regional Superintendent assumed the risk by executing the lease agreement without the assurance of knowing whether the financial and legal obligations are met. The value added for the Regional Superintendent to execute the leases was not evident. An improperly executed lease agreement could result in rework due to errors and the client may lose confidence in the regional office.

The Division bears the risk and was accountable to ensure the lease agreements were executed properly. IAB recommends the lease agreement execution remain with the risk owner, the Division, to facilitate an accountable, transparent lease process and to minimize the financial and legal risk.

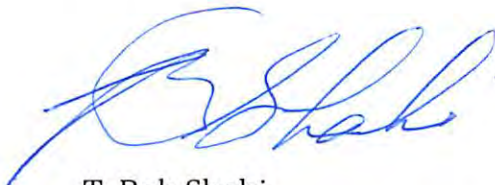
- c. The change in lease process has been communicated. Division staff conducted field visits to the regions to communicate and train regional staff on the new process. Written procedures were disseminated and available electronically. Management explained capacity issues were present in one region.

An internal quality assurance process, developed with the support of the Department's Director of Finance and Administration, would be useful tool for the Division to monitor and ensure consistent application of the lease process in compliance with Regulations.

Acknowledgement

We would like to thank the Division employees for their assistance and co-operation throughout this project.

Sincerely,



T. Bob Shahi
Director, Internal Audit Bureau
Finance

Enclosures

- c. Mr. Jamie Koe, Chair, Audit Committee
Ms. Brenda Hilderman, Director, Finance & Administration, Lands



Department of Lands
Commissioners Land Tenure Lease Application Process
Audit Period: As of February 2018

Date: June 7, 2018



Government of
Northwest Territories

Agenda

- 1.0 Introduction
- 2.0 Scope & objectives of the audit
- 3.0 Audit work performed & Conclusion
- 4.0 Findings/Areas to Consider
- 5.0 Next Steps



1.0 Introduction

- On April 1, 2014, Department of Lands was delegated to manage both Commissioner and Territorial Land.
- Commissioner's Land Administration Division (Division) in Yellowknife was responsible for the management and administration of the Commissioner's Land in accordance with the *Commissioner's Land Act (Act)*
- The Division was transitioning from regional to central administration of the lease application process.
- According to the Director, there were approximately 2,500-3,000 leases for Commissioner's land with revenue of about \$2.4 Million (2017-2018 Main estimates)



1.0 Introduction Contd.

Regions were classified as follows;

- Inuvik Region - Inuvik.
- Sahtu Region - Norman Wells.
- Deh Cho Region - Fort Simpson.
- North Slave Region - Behchoko and Yellowknife.
- South Slave Region - Fort Smith and Hay River.



2.0 Audit Scope & Objectives

2.1 Audit Scope

- Administration of Commissioner's Land after centralization of the lease application process as of February 2018
- Due to inadequate sample size, we were unable to test integrity of data relating to the lease administration

2.2 Audit Objectives

- Determine if Department of Lands has internal controls to administer land leases in compliance with the Act.



3.0 Work Performed

3.1 Key steps

- Reviewed procedures and documents available relating to the Commissioner's land lease application process. (Appendix A refers)
- Based on information obtained from North Slave, Sahtu, and Deh Cho, we performed a lease application process mapping. (Appendix B refers)
- We compared the results in Appendix A and B above.
- Held meetings with Regional Land Officers (RLOs) from North Slave, Deh Cho and Sahtu to discuss the process.
- Received and incorporated suggested changes from the RLOs in the process mapping.



3.0 Conclusion.

- Commissioner's Land lease application process was not uniform in the three regions.



4.0 Findings/Areas to consider .

4.1 Completion and submission of lease application with fees: (Appendix B Page 2 Note 1)

- Deh Cho Region – RLO completed applications together with applicants before submission.
- North Slave- Applicants usually called to establish if desired land was free before submitting application
- Sahtu- Lease application and fee submitted before establishing if desired land is free.

The reference manual for Lands Officer page 6 specifically deter RLO from completing application forms for clients due to possible perception of conflict of interest.



4.0 Findings/Areas to consider

4.1 (a) Recommendation:

RLOs must not complete application forms for clients so as to eliminate the perceived conflict of interest and comply with the reference manual designed by management.



4.0 Findings/Areas to consider

4.2 Execution of signed lease agreements: (Appendix B Page 4 Note 2)

- Deh Cho: Execution is carried out by Regional Superintendents at the region on behalf of the Commissioner.
- North Slave and Sahtu: Execution carried out by Director/Manager at Headquarters on behalf of the Commissioner .

Reference manual for Lands Officer requires execution of leases to be effected by the Manager or Director at Headquarters on behalf of the Commissioner and notify the RLO.



4.0 Findings/Areas to consider

4.2 (a) Recommendation:

All regions should follow the centralized lease application process as documented on pages (11-12) of the reference manual for Lands Officer.



4.0 Findings/Areas to consider

4.3 Dissemination of reference materials.

RLO Sahtu did not have access to reference materials relating to:

- Finance & Administration Procedural Manual,
- Reference Manual for the Lands Officer and
- the Lease Application Process flowchart (made by HQ)

RLOs should have access to reference materials for guidance and decision making.



4.0 Findings/Areas to consider

4.3 (a) Recommendation:

Management should ensure that all RLO have direct access to reference materials for the land administration process.



5.0 Next Steps

- Draft final report for review and feedback from Lands Management before submission to DM Lands.
- Management to review the lease application process to being used in all regions and ensure compliance with the centralised process.
- Management to determine if an independent assessment of information is required by December 2018





Comments, Questions, Suggestions

Internal Audit Bureau

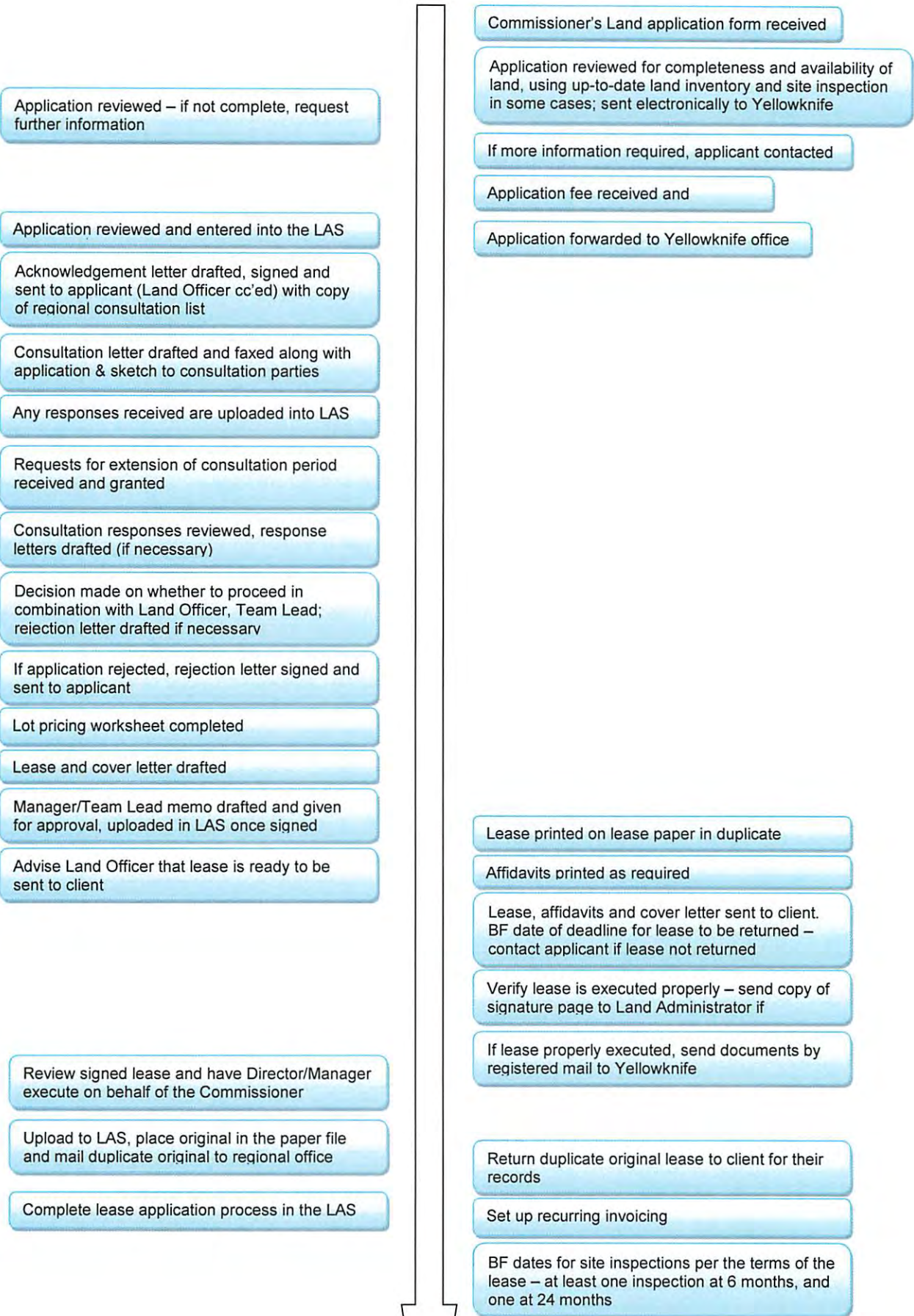


Government of
Northwest Territories

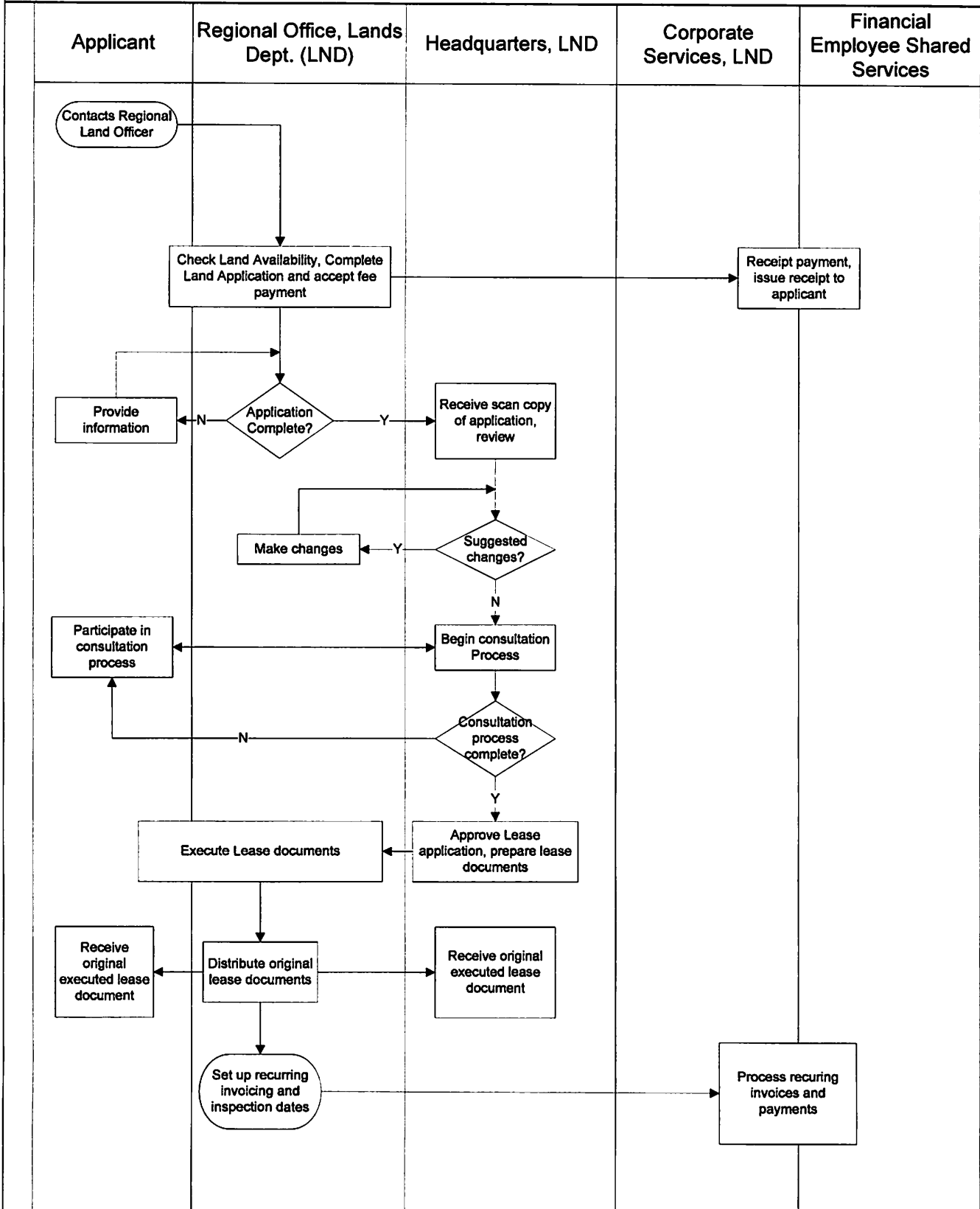
Lease Application Process

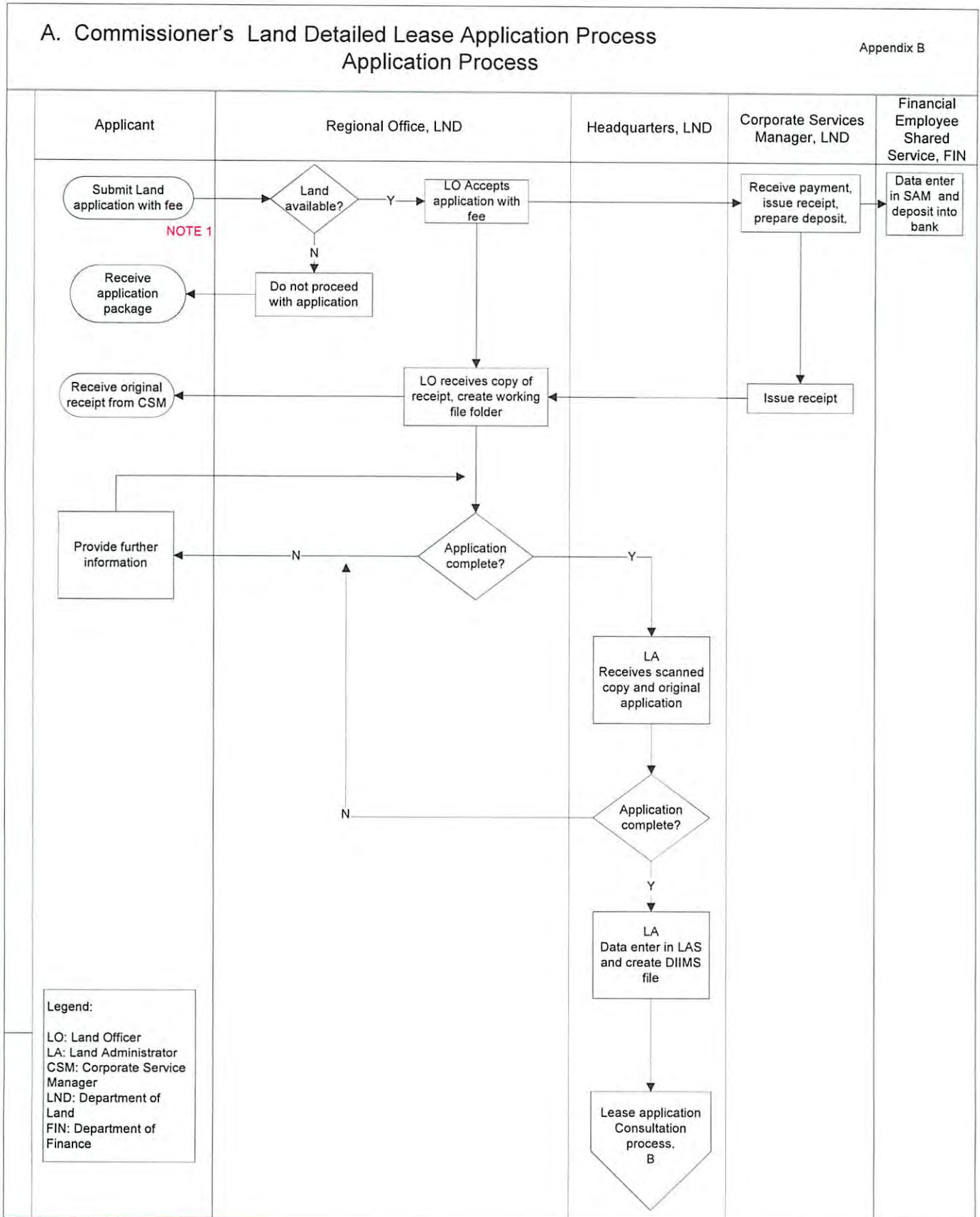
Land Administrator (YK)

Land Officer (Regional Office)



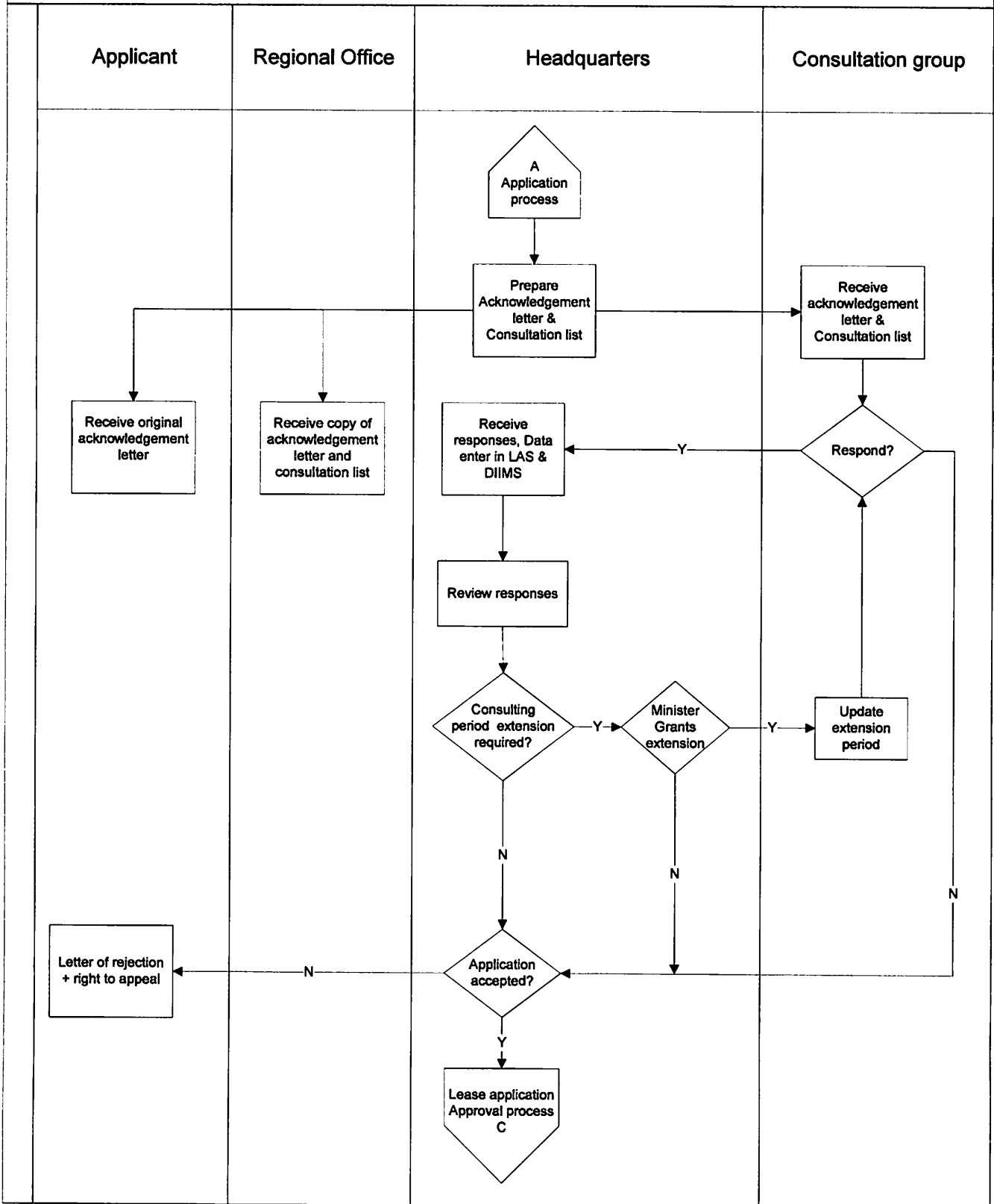
Commissioners Land Lease Application Process Overview





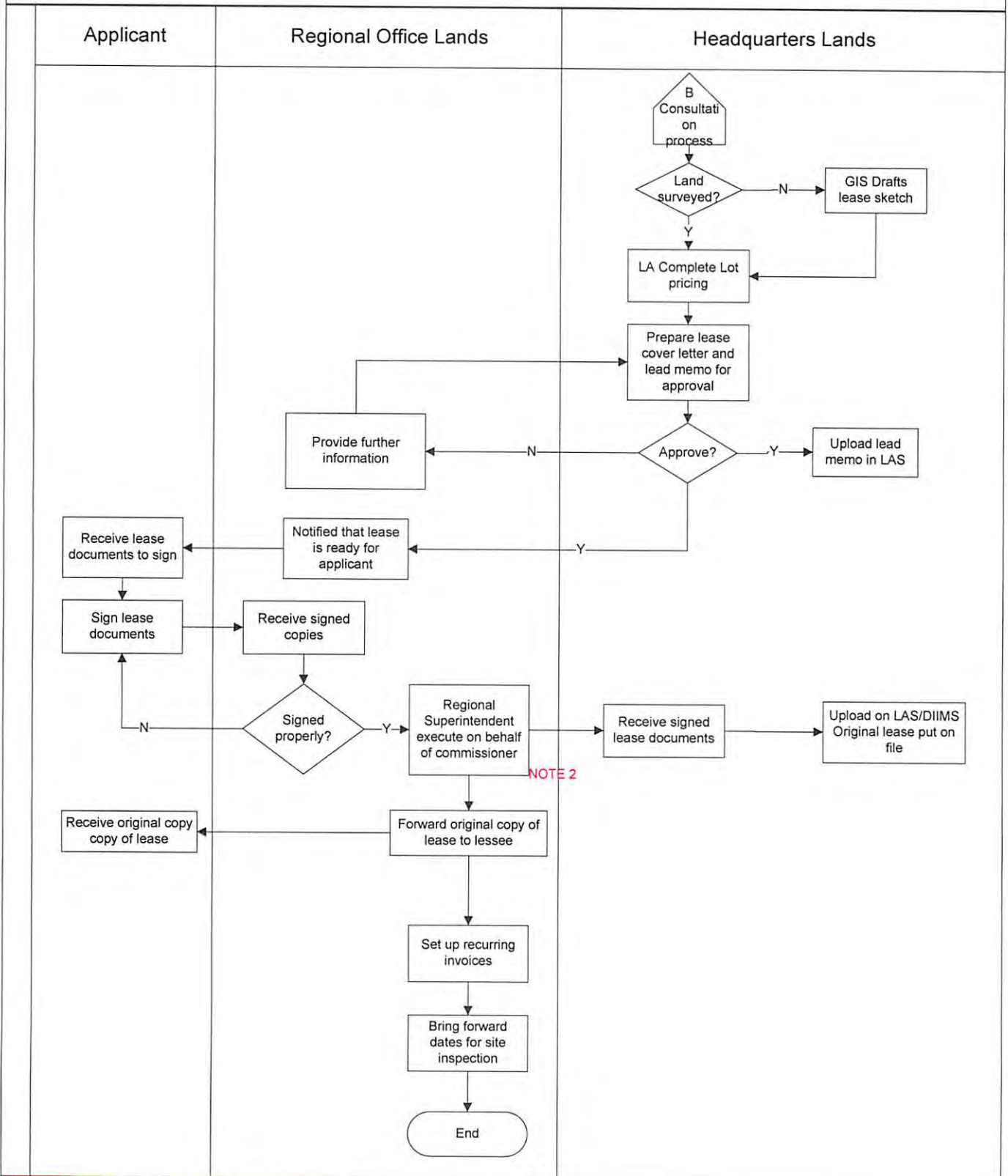
**B Commissioner's Land Detailed Lease Application Process
Consultation Process**

Appendix B



C: Commissioner's Land Detailed Lease Application Process
Approval Process

Appendix B



Note 1:

Applicant fills lease application with RLO as opposed to the centralized process mapping where RLO should receive and review lease applications submitted.

NOTE 2:

Lease execution is carried out by the Regional Superintendent on behalf of the Commissioner in Deh cho region as opposed to the centralized process mapping whereby lease execution should be effected by the Manager/Director at headquarters on behalf of the Commissioner.

North Slave and Sahtu, lease execution is carried out as defined in the centralized process mapping.