International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 09 Issue 10 October 2026

DOI: 10.47191/ijsshr/v9-i10-59, Impact factor- 8.361

Page No: 9085- 9094

The Authority of Indonesia's Information Commission to Review National Defense and Security Information Exemptions: A Public Accountability Perspective

Muhammad Bagaskara Rizqy Harmadi[1], Hasyim Asy'ari, S.H., M.Si., Ph.D.[2]

[1,2]Faculty of Law, Diponegoro University, Indonesia

ABSTRACT: Public information disclosure is a fundamental principle of a democratic state, intended to guarantee the public's right to access information and promote accountability in government administration. This principle is regulated under Law Number 14 of 2008 concerning Public Information Disclosure, which requires public bodies to provide access to public information. Nevertheless, the law also establishes exceptions for certain categories of information, including information relating to national defense and security. In practice, the boundary between information that must remain confidential to protect national security and information that serves a legitimate public interest is often unclear. This condition may lead to information disputes and create opportunities for public bodies to interpret information exemptions excessively. This study aims to analyze the authority of the Information Commission to examine exempted public information relating to national defense and security and to formulate a model for strengthening that authority to ensure information disclosure and public accountability. This research employs a normative legal method using statutory and conceptual approaches through an examination of legislation, legal doctrines, and relevant literature on public information disclosure and defense law. The findings indicate that strengthening the Information Commission's authority requires improvements to the classification system for defense information, reinforcement of harm and public interest tests, the implementation of closed examination procedures, and greater transparency regarding defense policy information that does not concern operational matters. These measures are expected to establish a more proportionate balance between protecting national security interests and safeguarding the public's right to information within a democratic system of government.

KEYWORDS: Public Information Disclosure, Information Commission, Exempted Information, National Defense and Security.

I. INTRODUCTION

The relationship between the state and its citizens is fundamentally shaped by the responsibility of public institutions to protect collective interests while ensuring the exercise of individual rights. In constitutional theory, the state represents a continuing political and legal organization, whereas the government exercises public authority within a particular institutional and political framework. This distinction is significant because governmental authority must ultimately serve the broader purposes of the state rather than the interests of those temporarily holding political power (Asshiddiqie, 2010). Accordingly, the legitimacy of governmental action depends not only on the lawful exercise of authority but also on the extent to which public institutions remain accountable to the people. Within this framework, transparency constitutes an essential element of democratic governance, enabling citizens to understand, evaluate, and scrutinize decisions made in the exercise of public authority.

Access to public information plays a central role in establishing such accountability. Information enables citizens to participate meaningfully in public affairs, assess governmental policies, and exercise oversight over institutions entrusted with public responsibilities. Without adequate access to information, public participation may become limited to formal democratic procedures, while the substantive processes underlying governmental decisions remain beyond meaningful public scrutiny. Suryani (2017) identifies public information disclosure as an important component of good governance, particularly in strengthening the relationship between public institutions and the communities they serve. Similarly, Trisakti et al. (2022) examine the relationship between transparency and the public interest, highlighting the significance of openness in the administration of public affairs. From this perspective, access to information is not merely an administrative service but an institutional mechanism through which governmental responsibility can be examined and public accountability can be maintained.

In Indonesia, the legal foundation for public information disclosure is principally established by Law Number 14 of 2008 concerning Public Information Disclosure (the Public Information Disclosure Law). Article 2(1) provides that public information

is generally open and accessible to users of public information, while Article 2(2) establishes that exemptions must be strict and limited. These provisions reflect a presumption in favor of disclosure, under which public bodies are expected to provide access to information unless a legally recognized ground for withholding it applies. The framework is also consistent with Law Number 25 of 2009 concerning Public Services, which recognizes openness and accountability among the principles governing public service delivery. Together, these legislative instruments place transparency within the broader obligations of public administration and reinforce the understanding that access to information serves both individual rights and the public interest.

Nevertheless, the right to access public information is not absolute. Certain categories of information may legitimately require protection where disclosure would threaten legally recognized interests. Article 17 of the Public Information Disclosure Law establishes several grounds for exemption, including information whose disclosure could endanger national defense and security under Article 17(c). The justification for such protection lies in the potentially serious consequences of revealing sensitive information concerning military operations, defense strategies, intelligence activities, or national security capabilities. Information of this nature may expose operational vulnerabilities or compromise the effectiveness of national defense measures. As discussed by Saputro and Satriya (2023), the application of public information disclosure principles within the Indonesian National Armed Forces raises particular legal questions concerning the protection of state confidentiality. Consequently, the legal treatment of defense-related information requires a careful distinction between material whose disclosure would create a genuine security risk and information whose confidentiality cannot be justified solely by its association with a defense institution.

The distinction is especially important because national defense institutions perform functions that extend beyond strictly operational military activities. Defense-related governance also involves public expenditure, institutional administration, resource allocation, and the formulation of policies that may directly affect civilian communities. Information concerning the general direction of defense policy, the use of public funds, or the legal framework governing public participation in national defense may therefore have significant implications for democratic oversight. At the same time, particular details concerning military capabilities, strategic deployment, and operational readiness may require continued protection. The central legal question is not whether all defense-related information should be disclosed or withheld, but how the boundaries between legitimate confidentiality and public accountability should be determined. Treating every document associated with national defense as inherently confidential risks extending statutory exemptions beyond their intended purposes and weakening the principle of limited disclosure restrictions.

Indonesian law addresses this tension through a consequence-based assessment of information exemptions. Article 2(4) of the Public Information Disclosure Law requires consideration of the consequences arising from disclosure and whether withholding information protects a greater interest than making it available to the public. This provision establishes an important legal basis for examining the justification for confidentiality rather than accepting an exemption merely because a public body has classified information as sensitive. The assessment must therefore consider the nature of the information, the interests potentially affected by disclosure, and the relationship between the anticipated harm and the applicable statutory exemption. In this context, an information exemption should operate as a legally justified limitation on access rather than as an unrestricted institutional discretion. The implementation of these principles is further supported by Information Commission Regulation Number 1 of 2021 concerning Public Information Service Standards, which provides a regulatory framework for the administration of public information services.

The implementation of information exemptions also requires an institutional mechanism through which disagreements over access can be examined independently. For this purpose, the Public Information Disclosure Law establishes the Information Commission as an independent institution responsible for implementing the statutory framework and resolving public information disputes. Under Articles 23 and 26, the Commission performs functions relating to public information service standards and the settlement of disputes through mediation and/or non-litigation adjudication. Its institutional position is particularly relevant when an applicant challenges a public body's decision to withhold information on the grounds of national defense or security. In such circumstances, the dispute extends beyond a procedural disagreement over access and raises a substantive question concerning the legal validity of the claimed exemption. The Commission must therefore operate within a framework that accommodates both the applicant's right to information and the public body's responsibility to protect legally confidential material.

Despite the existence of this legal framework, important questions remain concerning the scope and effectiveness of the Information Commission's authority when reviewing defense-related exemptions. The highly technical and sensitive character of national security information presents difficulties that may not arise in ordinary public information disputes. Evaluating a confidentiality claim may require consideration of operational risks, the sensitivity of particular documents, and the extent to which disclosure could reasonably affect protected defense interests. At the same time, excessive reliance on explanations provided by the public body withholding the information may undermine the independence of the review process. These concerns demonstrate the need to examine whether the existing statutory authority and procedural arrangements provide an adequate basis for assessing exemption claims while preserving the confidentiality of genuinely sensitive information.

The broader significance of this issue can be illustrated through policies involving both national defense interests and civilian participation. Indonesia's Law Number 23 of 2019 concerning the Management of National Resources for National Defense provides a legal framework for the involvement of national resources in the defense system, including the Reserve Component. Such policies create different categories of information that may require different legal treatment. Operational details relating to mobilization readiness or strategically sensitive personnel information may raise legitimate security concerns, whereas information regarding recruitment procedures, legal obligations, and protections afforded to participating citizens has a clear public accountability dimension. This distinction illustrates why the legal classification of defense-related information should be based on the content and consequences of disclosure rather than solely on the institutional origin of the information. It also demonstrates the importance of ensuring that legitimate security considerations do not unnecessarily restrict public scrutiny of policies affecting citizens.

These circumstances reveal a significant issue within the relationship between public information disclosure and the administration of national defense: the existence of statutory grounds for confidentiality does not, by itself, establish how those grounds should be reviewed in a particular dispute. Although Indonesian law recognizes openness as the general principle and confidentiality as a limited exception, the application of those principles to technically sensitive defense information raises questions about institutional authority, evidentiary assessment, and the appropriate limits of independent review. The legal problem therefore concerns not only the classification of exempt information but also the adequacy of the mechanisms available to determine whether a particular confidentiality claim satisfies the requirements of the Public Information Disclosure Law. Addressing this problem is essential to prevent unjustified restrictions on access while maintaining the protection required for national defense and security.

Against this background, this study examines the authority of Indonesia's Information Commission to review exemptions involving national defense and security information from the perspective of public accountability. It focuses on two interrelated questions: first, how the existing legal framework defines and regulates the Commission's authority to assess such exemptions; and second, how that authority may be strengthened to ensure a more accountable and legally consistent review process. Using normative legal research with statutory and conceptual approaches, the study analyzes the relationship between public information disclosure, national security confidentiality, and institutional accountability under Indonesian law. Its contribution lies in evaluating the adequacy of existing legal arrangements and identifying directions for strengthening the examination of defense-related confidentiality claims, with the aim of maintaining a proportionate balance between the protection of national security interests and the public's right to information.

This study employs normative legal research to examine legal norms, statutory rules, and conceptual principles governing public information disclosure and the boundaries of exempted information within the defense and security sector. To analyze these issues comprehensively, this study utilizes both a statute approach and a conceptual approach. The statute approach involves an examination of relevant legislative frameworks, notably Law Number 14 of 2008 concerning Public Information Disclosure, Law Number 23 of 2019 concerning the Management of National Resources for State Defense, and Law Number 3 of 2025 regarding the Amendment to Law Number 34 of 2004 concerning the Indonesian National Armed Forces, alongside pertinent administrative court rulings and Information Commission dispute decisions. Concurrently, the conceptual approach critically analyzes doctrines, theoretical views, and jurisprudence on state secrecy, civil-military relations, harm tests, and *in camera* review mechanisms (Mendel, 2008; Asshiddiqie, 2010; Ridwan, 2016; Widjajanto, 2022; Rahmat & Yusuf, 2023). The analysis also integrates comparative perspectives by examining the Freedom of Information regimes in the United States and the United Kingdom (United States Department of Justice, n.d.; Information Commissioner’s Office, n.d.). Legal materials consisting of primary, secondary, and tertiary sources were collected through documentary library research and regulatory tracking. These materials were subsequently analyzed qualitatively using grammatical, systematic, and teleological interpretations to evaluate the alignment between prevailing legal norms and defense governance practices, thereby formulating a normative framework to strengthen the Information Commission’s adjudicative authority.

II. DISCUSSION

A. EXISTING AUTHORITY OF INDONESIA'S INFORMATION COMMISSION TO REVIEW PUBLIC INFORMATION EXEMPTIONS RELATING TO NATIONAL DEFENSE AND SECURITY

The regulation of public information disclosure in Indonesia is fundamentally based on the principle that information held by public bodies should be accessible to the public, subject to limitations expressly recognized by law. Article 2(1) of Law Number 14 of 2008 concerning Public Information Disclosure establishes that public information is generally open and accessible to its users. This principle reflects the legal recognition that transparency is an essential component of democratic governance and that public institutions are accountable for the exercise of their authority. Nevertheless, the law does not establish an unrestricted right of access. Article 2(2) recognizes that certain information may be exempted from disclosure under strict and limited conditions.

The relationship between these provisions demonstrates that openness constitutes the general rule, while confidentiality must be supported by a legally justifiable exception.

One of the most sensitive grounds for restricting public access concerns information relating to national defense and security. Article 17(c) of the Public Information Disclosure Law provides an exemption for information whose disclosure could endanger national defense and security. This provision encompasses information associated with military strategies, defense capabilities, intelligence activities, operational planning, and other matters whose disclosure could compromise the protection of national interests. Within this framework, the legitimacy of confidentiality depends on the consequences associated with disclosure rather than merely on the institutional origin of the information. Saputro and Satriya (2023), in their discussion of public information disclosure within the Indonesian National Armed Forces, address the relationship between openness and the protection of state confidentiality. Their work illustrates the particular complexity of applying general transparency principles to institutions responsible for safeguarding national security.

The legal framework governing defense information must also be understood in relation to the legislation regulating the Indonesian National Armed Forces, commonly referred to as the TNI. Law Number 34 of 2004 concerning the Indonesian National Armed Forces, as amended by Law Number 3 of 2025, establishes the institutional position and principal responsibilities of the TNI within Indonesia's national defense system. The armed forces are responsible for protecting state sovereignty, maintaining territorial integrity, and defending the nation against military and armed threats. These responsibilities necessarily involve the management of strategically sensitive information, including operational capabilities, military deployment, defense planning, and intelligence-related activities. Disclosure of such information may create risks to military preparedness and national security. However, the institutional responsibility to safeguard sensitive information does not necessarily mean that every document produced or controlled by a defense institution qualifies for exemption under the Public Information Disclosure Law.

This distinction is significant because defense institutions also undertake administrative activities and participate in public policies involving state resources. The classification of information should therefore take account of the nature, purpose, and potential consequences of disclosure. Documents concerning operational readiness may require a different level of protection from those dealing with general institutional administration or public expenditure. Where information relates principally to the administration of public resources, an assertion of national security confidentiality should be supported by a demonstrable connection between its disclosure and the protected defense interest. Otherwise, there is a risk that the institutional status of a public body could be treated as sufficient justification for restricting information that remains relevant to public accountability. The legal challenge lies in maintaining the confidentiality of strategically sensitive material without extending exemptions to information that does not meet the applicable statutory requirements.

The importance of this distinction becomes apparent in the context of defense equipment procurement. The acquisition of military equipment involves the allocation of public financial resources and the implementation of governmental procurement policies. From an accountability perspective, information relating to general procurement policy, expenditure, and administrative decision-making may be relevant to public oversight. Nevertheless, defense procurement may also involve technical specifications, weapons-system capabilities, operational vulnerabilities, and strategic information whose disclosure could create security risks. Consequently, procurement-related information cannot be assessed as a single category for disclosure purposes. Each type of information must be considered according to its content and the potential harm arising from disclosure. This approach recognizes that public financial accountability and legitimate defense confidentiality may coexist within the same governmental activity.

A similar issue arises when the TNI participates in governmental programs that are not primarily concerned with military operations. The source article identifies the involvement of military institutions in activities associated with the Red and White Village Cooperative program as an illustration of the potential overlap between defense institutions and civilian economic policies. From a public administration perspective, information regarding the objectives, financing arrangements, procurement procedures, and implementation of an economic development program may carry a substantial public accountability interest. The participation of a military institution does not, in itself, establish that all information associated with the program concerns national defense secrets. The relevant legal question is whether disclosure of particular information would produce consequences falling within the statutory grounds for exemption. Accordingly, the classification of information should distinguish between activities that directly implicate defense security and administrative functions undertaken in support of broader governmental programs.

The management of the Reserve Component provides another illustration of the relationship between national defense confidentiality and public access to information. Law Number 23 of 2019 concerning the Management of National Resources for National Defense establishes a legal framework for the involvement of national resources, including citizens, in supporting the national defense system. Within this framework, information concerning recruitment requirements, the legal status of participants, applicable obligations, and available legal protections has a significant public interest dimension. Citizens affected by such policies have a legitimate interest in understanding their legal implications and the responsibilities imposed upon them. At the

same time, information concerning strategic personnel distribution, operational mobilization plans, or particular defense capabilities may raise genuine security concerns. The distinction between these categories demonstrates that the determination of confidentiality requires an assessment of the information itself rather than a general assumption that all matters connected with the Reserve Component must remain undisclosed.

The application of these legal distinctions is closely connected with the institutional authority of the Information Commission. Article 23 of the Public Information Disclosure Law establishes the Commission as an independent institution responsible for implementing the law and its implementing regulations, establishing technical guidelines for public information service standards, and resolving public information disputes through mediation and/or non-litigation adjudication. Its statutory functions are further regulated under Articles 26 and 27. In disputes concerning information withheld on national defense or security grounds, the Commission provides an institutional mechanism for examining whether a public body's refusal to disclose information is consistent with the applicable legal framework. Its authority is therefore not confined to facilitating communication between information applicants and public bodies. Through non-litigation adjudication, the Commission may also assess the legal justification presented for withholding the disputed information within the scope of its statutory powers.

An essential element of the exemption framework is the requirement to examine the consequences of disclosure. Article 2(4) of the Public Information Disclosure Law provides that the justification for exempting information must be considered carefully in light of the consequences arising from disclosure and the public interests involved. Article 19 further requires public bodies to undertake a consequence assessment before determining that particular information should be withheld from public access. This obligation is particularly relevant to defense-related information because the potential harm associated with disclosure may vary substantially according to the nature of the information and its operational significance. Information Commission Regulation Number 1 of 2017 concerning Public Information Classification further regulates the classification process and the examination of consequences. These provisions establish a normative basis for requiring confidentiality decisions to be supported by legal reasoning rather than by an unsupported declaration that particular information is sensitive.

From an institutional perspective, however, the existence of a statutory consequence assessment does not eliminate the difficulties associated with reviewing defense-related exemptions. The Information Commission must examine disputes involving information that may require specialized knowledge of military operations, defense systems, or national security risks. A public body may possess substantially greater technical knowledge concerning the disputed information than the applicant or the institution reviewing the exemption. Such informational asymmetry may complicate the assessment of whether the claimed security risk is sufficiently connected to disclosure. At the same time, accepting confidentiality claims solely because they originate from a defense institution would weaken the independent review function established under the Public Information Disclosure Law. The effectiveness of the Commission's authority therefore depends on its capacity to examine the legal grounds for withholding information while respecting the protection required for genuinely sensitive material.

A comparative perspective demonstrates that other jurisdictions also recognize the need to reconcile public access to governmental information with the protection of national defense. In the United States, the Freedom of Information Act establishes a general framework for accessing federal agency records while recognizing exemptions for protected interests. Exemption 1 addresses information properly classified under an executive order in the interests of national defense or foreign policy. As explained in the United States Department of Justice's guidance on the Freedom of Information Act, the protection applies to information that satisfies the applicable legal requirements for national security classification (United States Department of Justice, 2022). This framework illustrates an approach in which the legal validity of classification is significant to the determination of whether information may be withheld. Nevertheless, the American system must be understood within its own statutory and institutional structure and cannot be treated as directly equivalent to the authority exercised by Indonesia's Information Commission.

The United Kingdom adopts a different framework under the Freedom of Information Act 2000. Section 26 recognizes an exemption where disclosure would, or would be likely to, prejudice national defense or the capability, effectiveness, or security of the armed forces. Unlike an automatic exclusion based solely on the subject matter of defense, this provision requires consideration of the potential prejudice arising from disclosure. Furthermore, the defense exemption is subject to a public interest test, under which the interests supporting continued confidentiality must be assessed against the public interest in disclosure. The United Kingdom's Information Commissioner's Office explains that the application of Section 26 involves an examination of the relevant harm, the causal relationship between disclosure and that harm, and the likelihood of prejudice occurring (Information Commissioner's Office, 2023). This approach provides a useful comparative reference for understanding how legal systems may distinguish legitimate national security restrictions from unjustified limitations on public information access.

The comparison between Indonesia, the United States, and the United Kingdom demonstrates that national security exemptions may be structured through different legal mechanisms while addressing a common regulatory challenge. The United States emphasizes compliance with the requirements governing the classification of national security information, whereas the United Kingdom's defense exemption expressly incorporates an assessment of prejudice and the public interest. Indonesia, through the

Public Information Disclosure Law, recognizes openness as the general principle and requires consideration of the consequences associated with withholding or disclosing information. These approaches cannot be equated institutionally, particularly because the powers and procedures of the respective oversight bodies differ. Nevertheless, they demonstrate the importance of legally identifiable criteria when determining whether information concerning national defense should remain confidential.

Based on the existing Indonesian legal framework, the Information Commission possesses statutory authority to resolve disputes involving public information exemptions, including those concerning national defense and security. The principal issue is therefore not the complete absence of institutional authority, but the extent to which existing legal provisions and procedural mechanisms enable the Commission to review confidentiality claims effectively. Defense-related information presents particular difficulties because the protection of military and strategic interests must be reconciled with the public's right to scrutinize policies, expenditure, and governmental responsibilities. The existing framework provides a legal basis for this assessment through the principles of limited exemptions, consequence testing, and independent dispute resolution. However, the practical adequacy of that framework remains an important subject of normative examination, particularly in determining whether confidentiality claims can be assessed consistently without compromising protected security interests. This condition establishes the basis for considering how the Commission's review mechanisms may be strengthened to promote public accountability while maintaining legitimate national defense and security protections.

B. *NOTES ON IMPROVING THE AUTHORITY OF THE INFORMATION COMMISSION IN REVIEWING EXEMPTED INFORMATION RELATED TO NATIONAL DEFENSE AND SECURITY*

Strengthening the authority of the Information Commission to examine exempted information regarding state defense and security must focus on establishing a review mechanism capable of balancing public transparency with the protection of strategic state interests. The fundamental issue involves not merely the Commission’s formal statutory power in dispute resolution, but also the manner in which that power is exercised, the ways public bodies substantiate their exemption claims, and how the panel of commissioners determines whether access restrictions are legally justifiable (Ashari et al., 2019). Therefore, institutional enhancement cannot rely merely on abstract mandates; it requires procedural refinements across examination stages, evidentiary standards, technical expert consultation, and decision enforcement.

Within the Indonesian legal framework, the foundation for such improvements resides in Law Number 14 of 2008 on Public Information Openness (UU KIP). Article 2 establishes disclosure as the fundamental principle, subject only to strict and limited exceptions. Article 17 sets out categories of exempted information, including data that could jeopardize national defense and security upon release. Furthermore, Article 19 requires public bodies to conduct consequence tests meticulously before declaring information exempt, while Articles 23 and 26 delineate the Information Commission’s jurisdiction in dispute adjudication. These statutory provisions affirm that exemption determinations are not insulated from legal scrutiny but must remain justifiable under relevant legal standards.

Nevertheless, statutory provisions do not automatically ensure that exemption claims receive substantive review. In defense- and security-related disputes, public bodies possess substantial informational advantages because they control the contested documents, comprehend the technical context, and foresee potential risks of disclosure. Conversely, information requesters lack access to the disputed records, making it difficult to challenge the grounds for refusal. This imbalance places the Information Commission in a difficult position whenever proceedings depend solely on the public body’s unilateral assertions without adequate verification mechanisms. Procedural reforms must therefore enable independent scrutiny of confidentiality claims while continuing to safeguard information that is legitimately protected by law.

One fundamental step is strengthening substantive examination through *in camera* review. This closed examination allows the panel of commissioners to inspect contested records without disclosing their contents to the public during proceedings. Such an approach is necessary because assessing an exemption cannot rely solely on document titles, internal classifications, or written statements from public bodies. The Commission requires a sufficient evidentiary basis to determine whether a document’s substance falls strictly under statutory exemptions or merely contains administrative and policy details that should remain open to the public. For example, when an information request concerns defense procurement records, the dossier may include contract values, implementation timelines, payment terms, vendor identities, technical specifications, and specific operational configurations. Classifying an entire dossier as confidential simply because it touches upon defense is legally inappropriate; conversely, releasing the material in its entirety without prior inspection presents risks if technical components expose defense vulnerabilities or operational capabilities (Rahmat & Yusuf, 2023). Through *in camera* review, the panel can distinguish portions that are legitimately exempt from non-sensitive sections.

Implementing this mechanism requires identifying the disputed objects specifically. The public body must delineate the requested documents, specify sensitive components, state the statutory grounds for exemption, and explain why the information cannot be provided. The records must then be examined by the panel under applicable procedural laws and information security guidelines. To ensure accountability, every instance of access to sensitive documents must be recorded, examined copies must be

tightly controlled, and findings must be articulated in legal reasoning. Such legal reasoning does not need to expose protected substantive secrets, but it must explain the legal basis and justify why disclosure or nondisclosure complies with prevailing laws.

Developing *in camera* reviews must also respect the Information Commission's jurisdictional limits. The procedure cannot be construed as an unfettered mandate to inspect all state secrets or access classified defense information networks. Its application must conform strictly to the UU KIP and procedural regulations governing information dispute resolution. Should compulsory access powers require additional statutory backing, they must be established through appropriate legal instruments, ensuring that *in camera* examinations serve as an independent review mechanism rather than an unauthorized expansion of institutional authority.

Substantive review must further be supported by standardizing the consequence test. Although Article 19 of the UU KIP obligates public bodies to conduct consequence tests prior to declaring information exempt, consistent application requires clear guidelines outlining the specific factors to evaluate when assessing the impacts of disclosure. Such guidance is crucial because defense risks cannot always be proven through prior actual harm, but neither can they rest solely on abstract possibilities or speculative conjectures detached from the requested information.

The consequence test must begin with a precise identification of the withheld information rather than a general institutional label or file title. The public body must specify the withheld portions and map them directly to the statutory exemption categories under Article 17 of the UU KIP or other relevant legislation. The public body must then elaborate the anticipated consequences of disclosure, including the potential exposure of defense vulnerabilities, heightened risks to military personnel, or disruptions to ongoing operational patterns. This explanation must establish a direct and rational connection between disclosure and the anticipated threat, preventing generic assertions regarding national stability from being accepted without testable arguments.

Risk assessments must also incorporate relevant contexts, such as the data's currency, operational nature, public availability, and any changed circumstances affecting its sensitivity. Information concerning active operations carries different consequences compared to concluded activities. Similarly, individual data points that appear non-sensitive in isolation may generate operational vulnerabilities when combined with other available information. Consequently, evaluating documents in isolation is insufficient without analyzing how the information could be utilized in context.

To preserve consistency, the Information Commission can develop a standardized rubric that details the statutory basis, information identity, harm analysis, causal relationship, and possibilities for partial release. This instrument guides systematic examination by the adjudicators. Quantitative scoring formulas should not be the sole determinant, as assessing defense information involves legal and technical considerations that cannot be reduced entirely to numerical figures. The panel must ultimately weigh argument strength, evidentiary relevance, and statutory compliance.

Standardizing the consequence test requires strengthening evidentiary procedures. A public body claiming an exemption bears the burden of presenting sufficient evidence and justification for its refusal. This obligation does not mean that all underlying information must be disclosed to the requester, but rather that the grounds for withholding must be reviewable by the Commission through lawful proceedings. In matters involving sensitive files, review can occur *in camera*, while the requester receives an adequate explanation of the legal grounds without revealing protected content.

Requesters should not bear the burden of proving that disclosing records will not harm national security, as they lack access to internal defense records and expertise. Instead, requesters need only articulate the public interest motivating the request, such as auditing public expenditures, monitoring defense policies, or evaluating procurement accountability. These arguments must be weighed by the panel, although they do not automatically override statutory exemptions.

Throughout evidentiary proceedings, the Information Commission must evaluate whether an exemption is supported by applicable legal standards, pertinent facts, and coherent justifications. Statements by public officials and expert testimonies must be assessed on their substantive merits rather than accepted uncritically. Where claims hinge on technical considerations, the panel must verify that the testimony establishes a cogent link between disclosure and the claimed risk, ensuring that evidentiary review functions as a substantive test rather than a procedural formality.

The need for technical clarity highlights the importance of expert consultations carried out while preserving the Commission's independence. Defense information frequently involves weapons technology, cybersecurity, communications infrastructure, and tactical nuances that cannot be addressed through legal analysis alone. The Information Commission may establish rosters of independent experts across defense studies, information technology, procurement, and access to information law.

These consultations must observe clear parameters. Experts may provide explanations regarding how specific disclosures could expose system vulnerabilities or infrastructure risks, but the legal determination of whether the material meets the criteria of Article 17 of the UU KIP resides exclusively with the panel of commissioners. Technical sensitivity is not identical to legal exemption, as records considered sensitive by defense institutions do not automatically satisfy statutory withholding standards.

To maintain neutrality, expert selection must evaluate professional competence, independence, relevant experience, and potential conflicts of interest. While input from the military or the Ministry of Defense is valuable for clarifying operational contexts, it cannot serve as the exclusive basis for adjudication whenever independent verification is required. The Commission

must systematically govern documentation, the handling of sensitive materials, and the use of expert statements within procedural law.

Substantive review must also be coupled with the principle of partial disclosure. This principle recognizes that a single document may contain sensitive information alongside materials whose disclosure presents no comparable risk. The presence of isolated confidential data does not justify withholding an entire dossier. This approach reflects the strict and limited exemption doctrine of the UU KIP, provided that severability is determined through careful assessment of individual segments and their relational context.

Operationally, public bodies must separate exempt sections from releasable components. Highly sensitive details, such as precise facility coordinates, technical configurations, or security patterns, can be redacted, while contract values, payment timelines, and budget accountabilities undergo separate risk appraisals. Administrative data is not automatically disclosable under all circumstances, but neither can it be withheld simply because related parts of a file are confidential. The Information Commission must ensure that redactions are not applied so excessively that the delivered documents lose substantive meaning. Where extensive redactions are applied, the public body must justify each individual deletion. Reviewing panels can compare unredacted originals against proposed redacted copies *in camera*. For electronic records, redactions must be technically irreversible to prevent data recovery from metadata or hidden layers.

For example, citizens seeking defense procurement records possess a legitimate public interest in tracking public expenditures and contract amounts. Concurrently, the file might contain technical blueprints that reveal defense vulnerabilities. Partial disclosure offers an equitable balance by releasing non-sensitive administrative data while withholding critical technical elements, with all line-item redactions grounded in statutory assessments rather than agency discretion.

Beyond dispute proceedings, strengthening the Information Commission's authority requires cultivating proactive disclosure among defense public bodies. Over-relying on individual access requests increases administrative backlogs and triggers avoidable disputes that can be prevented if routine institutional information is published systematically. Articles 7 and 9 through 11 of the UU KIP govern these proactive publication duties, spanning regular, immediate, and continuously available disclosures.

In the defense sector, proactive openness can be expanded through releasing general policy frameworks, operational budgets, performance summaries, and non-sensitive procurement listings. Information formats can be tailored; for strategic matters, data can be shared in aggregated summaries that satisfy democratic oversight without compromising classified parameters. Proactive openness does not seek to declassify all defense assets, but guarantees that non-exempt governance data is not hidden unnecessarily.

Executing this regime necessitates robust institutional collaboration between Information and Documentation Management Officers (PPID), legal counsel, internal inspectorates, and military technical units. The PPID administers access services, technical units evaluate operational risks, and legal counsel ensures statutory compliance. This framework requires periodic classification reviews, as informational sensitivity wanes with shifts in technology, concluded operations, or evolving geopolitical environments. Nonetheless, such re-evaluations must follow statutory criteria and cannot be treated as an automatic termination of classified status.

Finally, these mechanisms require institutional governance that guarantees inter-agency coordination, document security, and procedural certainty. The Information Commission must maintain standardized protocols for requesting files, managing submissions, handling classified materials, tracking access logs, and resolving procedural disputes. These rules can be codified through standard operational procedures or revised institutional regulations within the agency's statutory scope. Should coercive discovery powers be deemed necessary, they must be anchored in explicit statutory amendments rather than inter-agency administrative protocols. This institutional strengthening must be complemented by capacity building and systematic case documentation. Commissioners and dispute staff need continuous training regarding access laws, security classifications, risk appraisal, and defense terminologies. At the same time, documenting precedents will harmonize interpretive consistency across rulings while ensuring that published opinions maintain necessary redactions to prevent secondary leaks of protected state secrets

III. CONCLUSIONS

The authority of the Information Commission to review exempted public information regarding national defense and security constitutes a vital instrument for balancing national security protection with the public's right to know. Although Law Number 14 of 2008 on Public Information Openness establishes a statutory basis for exempting information that could compromise defense and state security, its application must not rely solely on unilateral determinations by public bodies. Such exemptions must fulfill rigorous legal requirements, be substantiated by verifiable consequence testing, and consider tangible risks to protected state interests. In this context, the Information Commission serves a strategic role in preventing the arbitrary overclassification of information that undermines public oversight of governance and policymaking within the defense and security sectors.

Strengthening the Commission's authority requires refining the review mechanisms for exempted information. This entails developing measurable classification parameters for defense-related data, reinforcing consequential and public interest tests,

implementing *in camera* proceedings for genuinely sensitive materials, and expanding disclosure on defense policies that do not directly pertain to military operations or strategic state secrets. Furthermore, clear procedural regulations are necessary to delineate the scope of the Commission's review, establish standards for assessing confidentiality levels, and guide determinations on exempt status. These measures will enable the Information Commission to adjudicate disputes more effectively while respecting jurisdictional boundaries and national security imperatives. Consequently, state confidentiality can be safeguarded proportionately, while public transparency and institutional accountability remain upheld within a democratic state governed by the rule of law.

ACKNOWLEDGMENT

The author would like to express sincere gratitude to all parties who have contributed to the completion of this journal. The author also appreciates the valuable insights and support that have helped improve the quality of this research. Hopefully, this journal will contribute to the development of knowledge and serve as a useful reference for future research

REFERENCES

1) Ardiati. (2025). Peran Komisi Informasi Provinsi NTB dalam penyelesaian sengketa informasi publik di Komisi Informasi Mataram. *Jurnal Ilmu Sosial dan Pendidikan Lichen Institut (JISELI)*, 2(1), 1-6. https://jurnal.licheninstitute.org/index.php/jiseli/article/download/267/302
2) Aristotle. (1996). *Politics* (B. Jowett, Trans.). Oxford University Press.
3) Ashari, B., Ilmar, A., & Pide, A. S. M. (2019). Fungsi Komisi Informasi dalam mendukung proses informasi pertanahan di Kota Makassar. *Amanna Gappa*, 26(1), 39-52. https://doi.org/10.20956/ag.v26i1.6337
4) Asshiddiqie, J. (2010). *Pengantar Ilmu Hukum Tata Negara*. Rajawali Pers.
5) CNBC Indonesia. (2026). *Simak! Ini kriteria PNS yang bakal jadi Komcad militer*. https://www.cnbcindonesia.com/news/20260227154011-4-714595/simak-ini-kriteria-pns-yang-bakal-jadi-komcad-militer
6) Febriananingsih, N. (2012). Keterbukaan informasi publik dalam pemerintahan terbuka menuju tata pemerintahan yang baik. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 1(1), 135-156. https://doi.org/10.33331/rechtsvinding.v1i1.110
7) Information Commission of the Republic of Indonesia. (2017). *Information Commission Regulation Number 1 of 2017 concerning Public Information Classification*.
8) Information Commission of the Republic of Indonesia. (2021). *Information Commission Regulation Number 1 of 2021 concerning Public Information Service Standards*.
9) Information Commissioner's Office. (n.d.-a). *Freedom of Information Act 2000: Public Interest Test Guidance*.
10) Information Commissioner's Office. (n.d.-b). *Section 26-Defence*.
11) Kompas. (2026). *Impor 105.000 pikap untuk Koperasi Merah Putih ancam industri otomotif, pemerintah diminta batalkan*. https://www.kompas.id/artikel/impor-105000-pikap-ancam-industri-otomotif-nasional
12) Ma'ruf, S. A. (2025). Aktualisasi keterbukaan informasi publik pada era digital menurut kebijakan hukum terkait keterbukaan informasi publik. *Verfassung: Jurnal Hukum Tata Negara*, 4(1), 35-48. https://doi.org/10.30762/vjhtn.v4i1.682
13) Mendel, T. (2008). *Freedom of Information: A Comparative Legal Survey* (2nd ed.). UNESCO.
14) Puspitasari, I., & Triadi, I. (2024). Keamanan dan pertahanan dari aspek sistem keamanan nasional Indonesia. *Rechtsregel: Jurnal Ilmu Hukum*, 6(2), 131-140. https://doi.org/10.32493/rjih.v6i2.37480
15) Rahmat, R., & Yusuf, M. (2023). Tinjauan terhadap wewenang Komisi Informasi dalam menguji keputusan tata usaha negara. *Jurnal Litigasi Amsir*, 11(1), 70–78. https://journalstih.amsir.ac.id/index.php/julia/article/view/306
16) Republic of Indonesia. (2004). *Law Number 34 of 2004 concerning the Indonesian National Armed Forces*.
17) Republic of Indonesia. (2008). *Law Number 14 of 2008 concerning Public Information Disclosure*.
18) Republic of Indonesia. (2009). *Law Number 25 of 2009 concerning Public Services*.
19) Republic of Indonesia. (2019). *Law Number 23 of 2019 concerning the Management of National Resources for National Defense*.
20) Republic of Indonesia. (2025). *Law Number 3 of 2025 concerning the Amendment to Law Number 34 of 2004 concerning the Indonesian National Armed Forces*.
21) Ridwan HR. (2016). *Hukum Administrasi Negara*. Rajawali Pers.
22) Saputro, D. S., & Satriya, B. (2023). Penerapan asas keterbukaan informasi publik pada institusi Tentara Nasional Indonesia dikaitkan dengan data kerahasiaan negara. *MLJ Merdeka Law Journal*, 4(2), 101-111. https://doi.org/10.26905/mlj.v4i2.11529

23) Suryani, D. A. (2017). Mewujudkan good governance badan publik negara di Daerah Istimewa Yogyakarta melalui keterbukaan informasi publik. *Spirit Publik: Jurnal Administrasi Publik*, 12(1), 35-44. https://doi.org/10.20961/sp.v12i1.11736
24) Trisakti, F., Berliana, A. D. D., Al Bukhori, & Fitr, A. (2022). Transparansi dan kepentingan umum. *Jurnal Dialektika: Jurnal Ilmu Sosial*, 19(1), 29-38. https://doi.org/10.54783/dialektika.v19i1.61
25) Universitas Gadjah Mada. (2025, November 17). *Uji konsekuensi kunci menentukan sebuah informasi dikecualikan*. https://ugm.ac.id/id/berita/uji-konsekuensi-kunci-menentukan-sebuah-informasi-dikecualikan/
26) United Kingdom Parliament. (2000). *Freedom of Information Act 2000*, c. 36.
27) United States Congress. (1966). *Freedom of Information Act*, 5 U.S.C. 552, as amended.
28) United States Department of Justice. (n.d.). *Freedom of Information Act Guide: Exemption 1-Classified National Defense and Foreign Relations Information*.

There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non-Commercial 4.0 Intenational (CC BY-NC 4.0)
(https://creativecommons.org/licenses/by-nc/4.0/), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.