



LEGAL GOVERNANCE OF NON-CLASSIFIED INTELLIGENCE DISSEMINATION IN INDONESIA

Agustina Setianingrum^{1*}, Fuad Gani², Budi Wiweko³

^{1,2,3} Universitas Indonesia, Depok, Indonesia.

Email: agustina.setianingrum41@ui.ac.id

Abstract: Indonesia's freedom of information regime is built on a presumption of openness, while the national intelligence regime treats secrecy as the default means of protecting sources, methods, and operational safety. The resulting tension presents a legal problem that extends beyond a simple clash of principles, because the central issue is not only whether information may be disclosed, but also how the state designs lawful procedures to distinguish information that must remain protected from information that may be released in a safe and accountable form. This article asks how the policy characteristics, risks, and constraints of disseminating non-classified intelligence to the public can be understood in Indonesia. The study uses normative legal research through statutory and conceptual approaches, supplemented by qualitative document analysis of legal materials and recent scholarship on public intelligence, freedom of information, and information governance. The findings show that the core difficulty lies not merely in a conflict of norms, but in the absence of a procedural bridge linking the consequence-test logic of the disclosure regime with the protection logic of intelligence secrecy. This gap encourages over-classification, weakens accountability for disclosure decisions, and leaves little room for lawful and secure public intelligence products. The article proposes an Audit Ready Public Intelligence Disclosure (AR PID) model that structures non-classified intelligence dissemination through five auditable control points, allowing the protection of sources and methods to operate alongside legal compliance, public legitimacy, and stronger information governance.

Keywords: Freedom of Information Law; Information Policy; Information Governance; Intelligence; National Security.

INTRODUCTION:

Debates on freedom of information frequently return to a core question, namely how far the state can open information without harming national security. In Indonesia, this question becomes particularly complex because two statutory regimes operate with different default logics. The Freedom of Information (FoI) Law treats public information as presumptively open and requires consequence testing to justify exemptions. By contrast, the Intelligence Law makes secrecy a constitutive principle of intelligence work and attaches criminal sanctions to the unauthorised disclosure of intelligence secrets.¹

¹ Republik Indonesia, "Undang-Undang Nomor 14 Tahun 2018 Tentang Keterbukaan Informasi Publik"; Republik Indonesia, "Undang-Undang Nomor 17 Tahun 2011 Tentang Intelijen Negara."



Read in a narrow way, this overlap looks like a simple conflict between transparency and secrecy. This article advances a more operational reading. The normative tension is real, yet the more practical issue is the lack of an auditable governance process for releasing nonclassified intelligence to the public. This gap matters in a digital environment where threats move quickly, citizens expect evidence-based explanations, and misinformation can spread at scale through online channels.

In this article, nonclassified intelligence products refer to analytic outputs or early warning information that do not disclose sources, methods, personnel identities, or operational details. Examples include cyber threat bulletins, risk trend assessments on terrorism, summaries of disinformation threats, or security advisories with an educational purpose. In many cases, such outputs combine open-source intelligence with sanitised findings. This category differs from intelligence secrets, which Indonesian law defines broadly as information and documents connected to intelligence functions that must be protected.²

When no sector-specific guidance exists, policy practice tends to drift toward two extremes. One extreme is blanket secrecy that withholds even sanitised assessments that could support public resilience and meaningful participation. The other extreme is selective disclosure that resembles strategic communication while leaving weak accountability traces and creating incentives for narrative engineering. Recent state practices of publicly releasing intelligence in the Russia–Ukraine war illustrate both the strategic value of disclosure and the risk of instrumentalization.³

The research question addressed here asks what policy characteristics, risks, and constraints shape the dissemination of non-classified intelligence to the public in Indonesia. The article seeks to identify the legal and institutional features of that policy space, explain the risks and constraints that arise when intelligence is prepared for limited public disclosure, and develop a governance model that gives legal form to the dissemination of non-classified intelligence.

This article's novelty lies in reframing the dissemination of non-classified intelligence not merely as a matter of state communication, but as a problem of information governance that must satisfy legality, consequence-based review, procedural accountability, and auditable oversight. On that basis, the article proposes an Audit Ready Public Intelligence Disclosure (AR PID) model that connects the intelligence cycle to five governance control points, namely publication mandate, classification and consequence testing, sanitisation and analytic integrity, publication with metadata and retention, and oversight through audit trails and corrective review.

The article is organised as follows. After the introduction, the theoretical section explains how the article links information policy, FoI law, and intelligence studies. The method section describes the multi-method design. The results and discussion section presents policy characteristics, risks, constraints, and the proposed governance model. The conclusion summarises findings and implications.

² Republik Indonesia, “Undang-Undang Nomor 17 Tahun 2011 Tentang Intelijen Negara.”

³ Buluc et al., “When Spies Go Public! Lessons Learnt from the Instrumentalization of Intelligence for Strategic Communication in the Run-up to the Russian-Ukrainian War”; Dylan and Maguire, “Secret Intelligence and Public Diplomacy in the Ukraine War.”



THEORETICAL FOUNDATION AND ANALYTICAL FRAMEWORK:

This article draws on three strands of scholarship. The first concerns information policy and information governance. Information policy is understood as the set of normative and institutional choices that shape the lifecycle of information, from creation and processing to storage, dissemination, and use.⁴ In digital public administration, information governance requires clear roles, accountability, quality standards, and audit mechanisms so that decisions about information can be traced and evaluated (Abraham, Schneider, & vom Brocke, 2019; Fest, Wieringa, & Wagner, 2022).⁵

In practice, information governance problems are rarely limited to technical security. They also involve who is authorised to classify, who can release, how changes are documented, and how public trust is managed. In the security sector, these questions are amplified because information decisions can affect personnel safety and diplomatic relations. Audit trails therefore function as safeguards alongside technical controls.

The second strand covers freedom of information and national security exemptions. A recurring operational principle in Information Commission practice is maximum access with limited exemptions. The principle does not eliminate secrecy, but it requires proof that restricting access responds to a real and proportionate harm. Implementing regulations and service standards operationalise this logic through consequence testing and the possibility of partial disclosure by obscuring or blacking out exempt portions of the same document.⁶

The third strand comes from intelligence studies, particularly the intelligence cycle and contemporary practices of public intelligence disclosure. The intelligence cycle is conventionally described as a sequence of planning, collection, processing, analysis, and dissemination. Yet the literature also shows that the cycle is not always linear and may be shaped by politics, technology, and organisational culture. In some settings, public dissemination becomes an additional channel for awareness, advice, or co-production between the state and policy users.⁷

Recent work shows that states increasingly publish intelligence for strategic purposes, but the same practice raises risks of instrumentalisation and selective declassification when only favourable fragments are released.⁸ Legal scholarship further warns that selective declassification can manipulate accountability by allowing governments to release only what strengthens their preferred narrative.⁹

⁴ Pasek, "Defining Information Policy."

⁵ Abraham et al., "Data Governance"; Fest et al., "Paper vs. Practice."

⁶ Komisi Informasi Pusat, "Sejarah Komisi Informasi"; Komisi Informasi, "Peraturan Komisi Informasi Nomor 1 Tahun 2021 Tentang Standar Layanan Informasi Publik."

⁷ Petersen, "Three Concepts of Intelligence Communication"; Shakoar, "Unwinding the Intelligence Cycle in Denmark."

⁸ Buluc et al., "When Spies Go Public! Lessons Learnt from the Instrumentalization of Intelligence for Strategic Communication in the Run-up to the Russian-Ukrainian War"; Lefebvre, "State Secrecy."

⁹ Dudding, "Spinning Secrets: The Dangers of Selective Declassification."



The growth of open-source intelligence further changes the landscape. When parts of analysis derive from open sources, the possibility of public dissemination increases. However, the mixture of open and classified inputs in a single product can still generate inference risks. Sanitisation therefore requires more than removing names. It requires screening for deductive exposure of sources and methods.

The analytical framework links the intelligence cycle to the information lifecycle and to FoI procedures. Its core is an auditable disclosure governance model that treats public release of nonclassified intelligence as an additional dissemination path. The model introduces control points across the cycle. At each control point, key decisions must generate audit-trail artefacts that can be reviewed later, including legal basis records, source and method risk matrices, redaction rationales with consequence testing, tiered approvals, archiving metadata, and post-release monitoring reports.

Figure 1 summarises the framework by locating control points CP1 to CP5 along the intelligence cycle and the sanitised public release path.

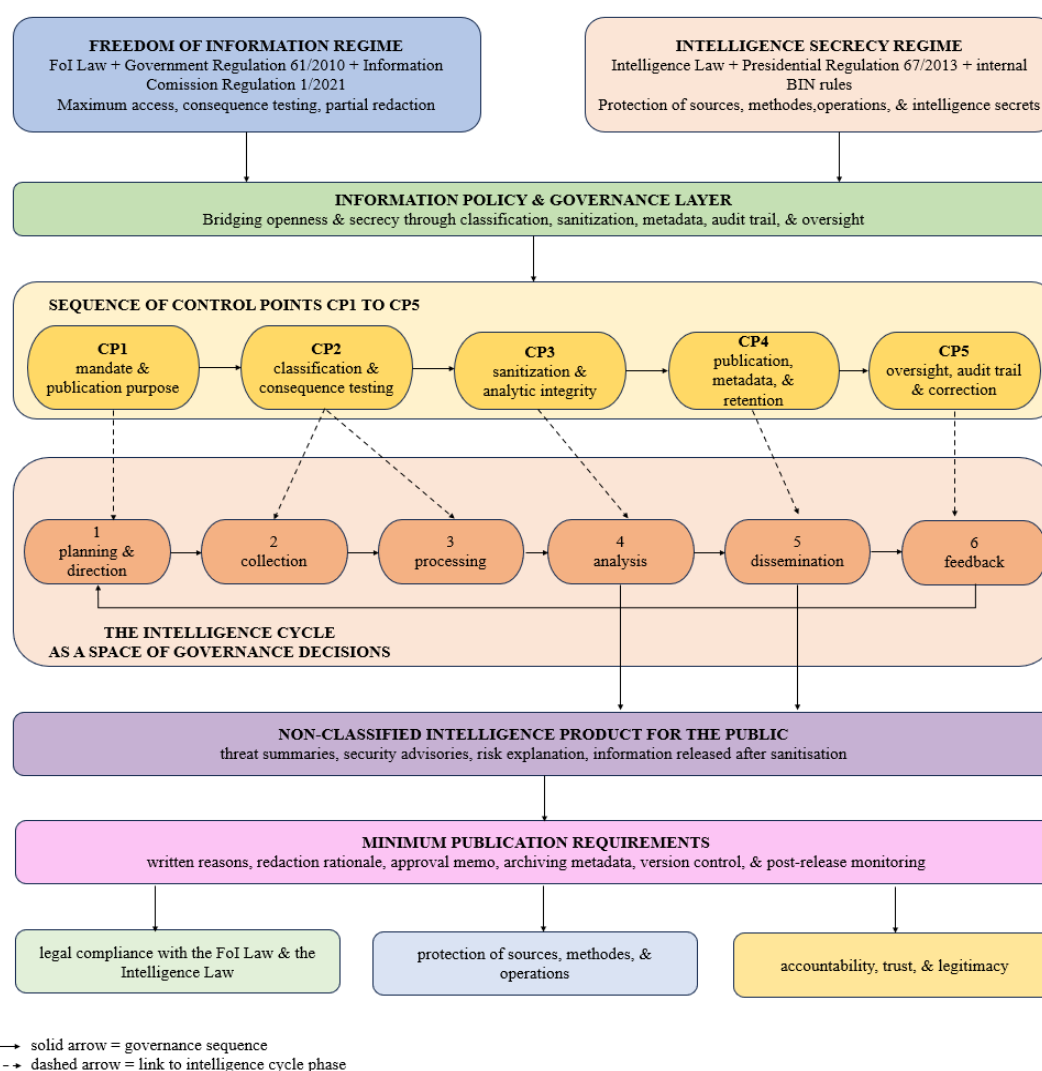


Figure 1. Conceptual framework of the Audit Ready Public Intelligence Disclosure (AR PID) model



METHODOLOGY:

The study adopts a multi-method research design suitable for a question that is both normative and operational. First, doctrinal legal research is conducted through statutory analysis, conceptual analysis, and harmonisation analysis to examine the relationship between the FoI Law, the Intelligence Law, and their implementing regulations. Second, qualitative document analysis is applied to the legislative background paper, public information service standards, and institutional documents relevant to information management practice. The analytic procedure follows a sequence of reading, extracting, analysing, and distilling findings in a systematic way.¹⁰

Documents were selected using two criteria. First, they had to directly address information access rules or intelligence secrecy rules. Second, they had to be publicly available so that the analysis can be replicated. This is not merely a practical choice. In an intelligence setting, public scrutiny depends on whether procedural rules are themselves visible, including classification grounds, consequence testing, partial disclosure techniques, and release recordkeeping. Where those procedural rules are absent from the public domain, refusals and disclosures risk turning into administrative habits rather than reviewable legal decisions. During analysis, texts were coded into three categories aligned with the research question, namely policy characteristics, risks, and constraints. Codes were then compared across documents to identify patterns and regulatory gaps.

Third, a limited comparative reading of recent scholarship on public intelligence disclosure is used to identify transferable risk patterns and governance lessons. Finally, a prescriptive conceptual design element is employed to develop an auditable disclosure governance model as the article's policy output, meaning a procedural model that can be adopted as internal guidance or standard operating procedures.

Primary legal materials include the Freedom of Information Law, the Intelligence Law, implementing regulations, and publicly available institutional documents. Secondary materials include peer-reviewed scholarship from the last five years on FoI, state secrecy, intelligence oversight, open-source intelligence, and information governance.

RESULTS AND DISCUSSION:

None.

Policy characteristics of nonclassified intelligence dissemination

Indonesia's Freedom of Information Law affirms a presumption of openness while listing strict exemptions, including information that could endanger defence and security, as well as intelligence strategies, operations, tactics, and capabilities. At the same time, the same law limits exemptions through the requirement of consequence testing and the principle that relevant exemptions are not permanent.¹¹

¹⁰ Morgan, "Conducting a Qualitative Document Analysis"; Dalglish et al., "Document Analysis in Health Policy Research."

¹¹ Republik Indonesia, "Undang-Undang Nomor 14 Tahun 2018 Tentang Keterbukaan Informasi Publik."



From a harmonisation perspective, these elements suggest that national security exemptions should operate as proven exceptions rather than as automatic labels. A product is not closed merely because it originates from an intelligence body. It is closed when it contains parts that satisfy a demonstrable harm threshold under consequence testing, or when it meets the definition of intelligence secrets under the Intelligence Law.

At the implementation level, the Government Regulation implementing the Freedom of Information Law operationalises consequence testing and requires public bodies to build information service systems. The Information Commission's service standards introduce partial disclosure through blacking out or obscuring exempt parts of the same document. In information policy terms, this rule recognises that a single information artefact may contain both open and closed elements. Good governance therefore does not choose between open and closed in a binary fashion, but manages calibrated openness responsibly.¹²

By contrast, the Intelligence Law defines intelligence secrecy broadly to include information, objects, personnel, activities, and documents connected to intelligence functions that must be protected. The law sets a retention period of up to twenty-five years and allows extension with parliamentary approval. Within that period, disclosure is framed as a highly limited exception, mainly for evidentiary purposes in closed court proceedings.¹³

The legislative background paper to the Intelligence Law notes that the Freedom of Information Law treats information related to intelligence as exempt information. This tendency may reflect a desire to protect sources and methods, yet it also creates a risk of blanket secrecy when intelligence products that could be released in sanitised form are treated in the same way as operational secrets.¹⁴

In the institutional regulatory landscape, a presidential regulation on intelligence coordination authorises intelligence organisers to establish intelligence secrecy classifications and to organise the intelligence system. At the same time, Badan Intelijen Negara (BIN) Regulation No. 01 of 2022 places the Directorate of Dissemination and Publication under the Deputy for Communication and Information as the unit responsible for dissemination and publication within the National Intelligence Agency.¹⁵ Within the same organisational cluster, the Directorate of Inter-Institutional Communication includes the Subdirector of Information and Documentation Management, which is functionally the closest unit to the mandate of a Public Information and Documentation Management Officer and is therefore the most plausible institutional home for the Information and Documentation Management Officer (IDMO or PPID/Pejabat Pengelola

¹² Republik Indonesia, "Peraturan Pemerintah Nomor 61 Tahun 2010 Tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik"; Komisi Informasi, "Peraturan Komisi Informasi Nomor 1 Tahun 2021 Tentang Standar Layanan Informasi Publik."

¹³ Republik Indonesia, "Undang-Undang Nomor 17 Tahun 2011 Tentang Intelijen Negara."

¹⁴ Sekretariat Jenderal DPR RI, "Naskah Akademik RUU Intelijen Negara Hasil Harmonisasi Baleg."

¹⁵ Badan Intelijen Negara, "Peraturan Badan Intelijen Negara Nomor 1 Tahun 2022 Tentang Organisasi Dan Tata Kerja Badan Intelijen Negara."



Informasi dan Dokumentasi) function within BIN. Nevertheless, no detailed sector-specific guidance appears in the public domain on how public product sanitisation should be linked to consequence testing, partial disclosure, and archival responsibility in the way developed under the FoI regime.¹⁶

A further finding concerns the choice to rely only on documents available in the public domain. This is not merely a practical limitation. It is consistent with the article's legal and governance focus. The problem under examination is public disclosure. For that reason, the most relevant materials are those norms, procedures, and organisational arrangements that can be known, interpreted, and relied upon by citizens, journalists, researchers, and oversight bodies. Internal rules may well shape actual practice, but if they are not publicly accessible, they cannot function as public standards of legality and accountability. In that sense, the visibility of procedural rules is itself part of the governance problem under study.

From an information governance perspective, publishing procedural rules on classification, release, redaction, and archiving performs a function beyond symbolic transparency. Publicly available rules clarify who decides, which criteria are used, how decisions are recorded, and under what conditions they may be reviewed. Without such procedural visibility, the public sees only the final outcome, either disclosure or refusal, while the legal rationality of the decision remains opaque. In intelligence settings this opacity carries a particular risk because secrecy can turn from a justified protective instrument into an unquestioned organisational habit that is insulated from meaningful scrutiny.

The institutional implication is equally important. If the Directorate of Dissemination and Publication serves as the release node, then the most plausible home for the Public Information and Documentation Management Officer within BIN lies in the Subdirectorate for Information and Documentation Management under the Directorate for Inter-Agency Communication. That placement is coherent because it sits within the Deputy for Communication and Information and is therefore close to documentation, institutional communication, and release archiving functions. At the same time, the PPID function in an intelligence environment cannot mirror the same role in an ordinary public body. It is better conceived as a restricted access PPID with layered review, working jointly with legal officers, information security officers, and classification authorities so that consequence testing is directly connected to the legally protected categories of intelligence harm.

Risks associated with public dissemination

The first risk is operational and relates to safety. Even when an output is labelled nonclassified, weak sanitisation can reveal traces of sources and methods or expose operational patterns that adversaries can recognise. Scholarship on intelligence disclosure shows that release, especially in

¹⁶ Republik Indonesia, "Peraturan Presiden Nomor 67 Tahun 2013 Tentang Koordinasi Intelijen Negara"; Badan Intelijen Negara, "Peraturan Badan Intelijen Negara Nomor 1 Tahun 2022 Tentang Organisasi Dan Tata Kerja Badan Intelijen Negara."



conflict settings, can function as a strategic instrument but may also invite retaliation, deception, and long-term damage to collection ecosystems.¹⁷

Operational risk also emerges through inference. Public release of analytic summaries can enable adversaries to infer specific sources through a combination of timing, granularity, and linguistic patterns, even if no source is explicitly named. Sanitisation therefore requires screening for deductive exposure, not merely removing identifiers.

The second risk concerns analytic integrity and selective declassification. Public release inevitably involves selection. Without documented standards, that selection may be driven by short-term political incentives rather than analytic discipline. Legal scholarship in the United States shows that selective declassification may create informational asymmetries that weaken accountability and disturb public trust. In this setting, an audit trail becomes essential for distinguishing disclosure grounded in security and public interest from disclosure aimed merely at mobilising support.¹⁸

The third risk is legal and rights-based. Public intelligence products may include personal data, profiling, or assessments with reputational consequences. With a stronger data protection agenda, uncontrolled dissemination may create new disputes and broaden distrust. Similar risks appear in debates on surveillance technologies in policing and the need for fair and accountable guidance.¹⁹

The fourth risk is digital security and integrity. Publishing intelligence products through online channels requires an adequate information security posture because cyberattacks may compromise content integrity, falsify documents, or exploit metadata. Recent research shows that online public services frequently contain security weaknesses with direct implications for trust and legitimacy. In governance terms, this risk requires robust metadata management, internal access controls, and post-release verification procedures.²⁰

In addition to these four risks, there is an epistemic risk that is often understated. A public intelligence product is not a neutral list of facts. It is an assessed judgment that may contain probability statements, confidence levels, and substantial uncertainty. If that uncertainty is suppressed for the sake of message simplicity, the public may receive a product that appears decisive but is analytically fragile. Over time, a failure to communicate the limits of the analysis can erode institutional legitimacy when predictions or assessments later change. For that reason, nonclassified intelligence dissemination should develop a public language that remains honest about evidentiary limits and confidence levels without exposing sensitive details.²¹

¹⁷ Buluc et al., “When Spies Go Public! Lessons Learnt from the Instrumentalization of Intelligence for Strategic Communication in the Run-up to the Russian-Ukrainian War”; Dylan and Maguire, “Secret Intelligence and Public Diplomacy in the Ukraine War”; Marleku, “Public Intelligence as a Strategic Tool.”

¹⁸ Dudding, “Spinning Secrets: The Dangers of Selective Declassification.”

¹⁹ Dolata and Schwabe, “Moving beyond Privacy and Airspace Safety.”

²⁰ Ribeiro et al., “Assessing the Information Security Posture of Online Public Services Worldwide.”

²¹ Petersen, “Three Concepts of Intelligence Communication”; Díaz-Fernández and Del-Real, “Measuring Trust in Intelligence Services.”



There is also a risk tied to interagency and international relationships. Intelligence products are often built from information shared across domestic institutions and sometimes across jurisdictions. Once information is released, the question is not only whether disclosure is safe for national interests, but also whether it breaches the confidence of partner institutions that supplied the information. In contemporary intelligence governance, interagency trust is an operational asset of high value. Nonclassified dissemination therefore requires scrutiny of origin and uses rights, not just scrutiny of substantive content.²²

At the socio-legal level, risk also arises when a public intelligence product concerns specific communities, regions, or threat narratives that carry political sensitivity. If wording is careless, release can produce labelling, reinforce stereotypes, or shift suspicion onto communities that should instead be protected. This matters because public intelligence is often justified in the name of collective safety, while in the absence of normative safeguards it can also widen the effects of stigma. Audit trails therefore serve not only to document redaction reasons, but also to demonstrate that non-discrimination and proportionality were considered in the review process.²³

Constraints in law and institutions

A first constraint is normative and stems from the absence of sector-specific procedures bridging FoI principles and intelligence secrecy. FoI law provides consequence testing and partial disclosure techniques, yet these are not translated into intelligence-specific workflows. Conversely, intelligence law protects secrets but does not specify how to distinguish product categories that can be released after sanitisation.

A second constraint concerns organisational culture. Intelligence practices rely on need-to-know and compartmentation. These practices are rational for operational security, but they complicate cross-unit processes required for sanitisation and public release, including coordination among analysts, information security officers, legal reviewers, and records managers. Without a clear process design, disclosure decisions tend to become ad hoc.

A third constraint relates to accountability and oversight. Scholarship on intelligence oversight in the digital age stresses that accountability depends on documentary traceability and on oversight mechanisms capable of assessing compliance with law and ethics. In Indonesia, intelligence oversight still operates largely through political channels and secrecy, so building an audit trail for public products introduces an additional institutional design challenge.²⁴

A fourth constraint concerns recordkeeping and archiving. Once released, a public intelligence product remains an organisational record with evidentiary value for evaluation, learning, and accountability. Without metadata standards, retention scheduling, and version control, publication may create disputes over authoritative versions, analytic context, and post-release changes. In FoI practice, archiving release records is also necessary to ensure consistent responses in future access requests or dispute resolution.

²² Dylan and Maguire, “Secret Intelligence and Public Diplomacy in the Ukraine War.”

²³ Juneau, “National Security Transparency and Relations with Minority Communities.”

²⁴ Constantino and Wagner, “Accountability and Oversight in the Dutch Intelligence and Security Domains in the Digital Age”; De Werd, “The Value of Engaged Critique.”



A further constraint lies in the disconnect between public information service logic and intelligence production logic. In many public bodies, the Public Information and Documentation Management Officer become involved after a document already exists. In intelligence settings that sequence is often too late because openness decisions should ideally be anticipated while the product is being built. If the PPID function only enters after the product is finalised, the institution tends to face two equally poor options, either a blanket refusal or a hurried and weak redaction exercise. This shows that the PPID role within BIN should be designed not merely as an administrative access channel, but as a governance node connected to production, review, and archiving from the outset.

A sixth constraint concerns cross professional capacity. Nonclassified intelligence dissemination requires collaboration among analysts, information security specialists, records professionals, communicators, and lawyers. Each group operates with a different internal logic. Analysts privilege accuracy and inference, security officers privilege exposure minimisation, communicators privilege clarity, and lawyers privilege authority and proportionality. Without a stable review forum, these differences can harden into informal vetoes that block release altogether. From an information policy standpoint, the difficulty demonstrates that disclosure governance is never purely technical. It is a question of role coordination and decision architecture.

A seventh constraint concerns the limited public visibility of secondary rules on classification and release practice in the intelligence sector. In many other sectors, the quality of governance can be assessed through the existence of service standards, operational guidelines, and openly available policy documents. In the intelligence sector, more detailed internal rules may well exist, yet if procedural rules are never made public, the public cannot assess which standards guide status changes, what safeguard's structure release decisions, or how corrections are made. This lack of procedural visibility is itself an information governance problem. Good governance requires not only the protection of sensitive substance, but also the intelligibility of the rules that govern that protection.

Auditable disclosure governance model

The proposed model combines maximum access with limited exemptions with the protection of intelligence secrecy through five control points aligned with the intelligence cycle (Figure 1). The model does not replace substantive intelligence authority. Instead, it forces disclosure processes to produce traceable artefacts that can support internal oversight, ethical review, and institutional evaluation.

CP1 establishes a publication mandate and legal basis. At the planning stage, public release should be framed as a legitimate public information need, for example early warning or risk mitigation. The artefact is a tasking record specifying purpose, scope, and legal references. This step matters to prevent disclosure from becoming a spontaneous act without accountability.



CP2 screens source, method, and personal data risks during collection and processing. Information receives initial risk labels and classification. The artefact is a risk matrix separating information that can be open, information that can be open after redaction, and information that remains restricted. This step includes an initial assessment of whether content approaches the legal category of intelligence secrets or remains at a lower sensitivity level.

CP3 protects analytic integrity and formalises sanitisation rationale. At the analysis stage, reasoning standards and traceability should be clarified without exposing sensitive details. The artefact is a redaction rationale sheet explaining what was removed and why, including a consequence testing summary. The sheet functions as a bridge between analytic standards and legal standards.

CP4 secures tiered authorisation and archiving. Before release, legal and information security reviews occur alongside approval by authorised officials. Artefacts include approval memoranda, release metadata, and an archiving package storing pre- and post-sanitisation versions. Version control becomes important to preserve consistency if updates are issued.

CP5 implements post-release monitoring. After publication, the organisation monitors misinformation, distortion, and unintended effects, and prepares correction mechanisms. Artefacts include monitoring reports, correction logs, and impact evaluations for security and public trust. Monitoring can also trigger clarifications to prevent misinterpretation.

Normatively, the model treats redaction and obscuration as a legal technique already recognised in FoI service standards. Applied to nonclassified intelligence products, the technique enables calibrated openness while protecting genuinely sensitive elements. Institutionally, the model supports the establishment of a specialised public information function with restricted access, capable of conducting consequence testing and managing release records professionally.

Viewed as an information governance architecture, the AR PID model shifts the central question away from the simple issue of whether information may be disclosed and toward the more mature question of how disclosure decisions are formed, tested, recorded, and reviewed. This shift matters because the conflict between openness and secrecy is rarely resolved at the level of abstraction. It has to be broken down into smaller decisions, each with an identifiable decision maker, legal basis, and documentary trace. In this model, legality does not stop at the level of statutory principle. It is translated into a workflow that can be reconstructed if a dispute, ethical concern, or policy review later arises.

At the first and second control points, the organisation is essentially building its evidentiary foundation. The publication mandate shows that release serves a lawful and defined purpose, while the risk matrix shows that the institution has actively considered source, method, personal data, and strategic harms. Together, these artefacts strengthen the legal position of release because the rationale for openness is always linked to a specific harm assessment. In future access disputes, records of this kind also make it easier to explain why some segments were released and others withheld without restarting the entire evaluative process.



At the third and fourth control points, the model addresses the area where selective declassification most often arises. The redaction rationale sheet does not merely list what was removed. It explains why removal was necessary and how that removal does not alter the core analytic meaning of the product. The approval memorandum and release metadata then show that the public version passed legal review, information security review, and tiered authorisation. The organisation can therefore demonstrate that publication was not the preference of a single official, but an institutional act that can be reconstructed and defended.

At the fifth control point, post release monitoring serves a function that legal discussions often understate. Many disputes do not arise when information is first released, but after that information is quoted out of context, reframed, or combined with other data. For that reason, monitoring of unintended effects should be treated as part of the duty of care rather than as a mere communications task. Correction logs, clarification notices, and updated versions help preserve informational integrity while showing that procedural transparency continues after release rather than ending at the moment of publication.

Implications and recommendations

First, sector-specific guidance is needed to define categories of nonclassified intelligence products suitable for public release, such as cyber threat bulletins, risk trend assessments, and early warning advisories that do not expose sources.

Second, integrating information policy thinking into intelligence practice requires standardised metadata, archiving, and version control for every release. Audit trails support oversight while also protecting the organisation from allegations of manipulation because sanitisation decisions are documented.

Third, to reduce politicisation risk, every public release should include minimal methodological context, such as confidence ranges, data limitations, and reasons why some details cannot be disclosed. Such contextualisation can enhance public trust without exposing operational secrets.

Fourth, normative harmonisation could be strengthened by clarifying that intelligence-related information is not automatically exempt in a blanket manner, but remains subject to consequence testing and partial disclosure when risks can be managed. This clarification need not weaken the secrecy principle. Rather, it specifies how secrecy operates when products are designed for public resilience.

Fifth, audit trails should be aligned with internal ethics and oversight processes. Audit artefacts should not be static records but inputs for organisational learning. Over time, such design can improve trust through procedural transparency rather than operational revelation.



As a regulatory matter, the most realistic short term option is an internal BIN regulation specifically governing nonclassified intelligence products, sanitisation procedures, consequence testing forms, and the storage of pre and post redaction versions. Such an instrument does not need to disclose substantive classification content or source lists. It does, however, need to be detailed enough for the public to know that release decisions follow a lawful procedure. Public visibility of procedural rules would actually strengthen the protection of genuine secrets because it would sharpen the distinction between information that remains classified and information that may be disclosed after sanitisation.

In the medium term, harmonisation could also be pursued through a joint protocol involving BIN, other security related bodies, and the Information Commission. Such a protocol would help bridge the gap between the logic of public information services and the logic of intelligence protection, especially in situations involving proactive release, access requests, or disputes. It would also clarify the coordination path linking the Directorate of Dissemination and Publication, legal review, information security functions, and the PPID role within BIN.

In the longer term, strengthening nonclassified intelligence dissemination should be understood as part of institution building and trust building. A state does not need to reveal operational secrets in order to enhance legitimacy, but it does need to show that secrecy decisions are made under lawful standards, consistent procedures, and meaningful oversight. The expanded discussion therefore underlines that the core problem is not whether the public may ever have access to intelligence related information. The deeper problem is the absence of a governance design that allows legitimate public needs to be met without sacrificing the protections that genuinely must remain in place.

CONCLUSIONS

This article shows that Indonesia's openness-secrecy paradox is better understood as a problem of legal governance that has not yet acquired an adequate procedural form. The freedom of information regime provides consequence testing and partial disclosure techniques, while the intelligence regime provides strict protection for intelligence secrets. Yet the point of convergence, namely a defensible procedure for sanitising and releasing non-classified intelligence products, has not been clearly established. As a result, over-classification remains the dominant institutional response and the space for calibrated openness remains narrow.

In answering the research question, the current policy characteristics reveal a strong default towards secrecy without sufficient operational guidance for calibrated openness. The most salient risks include source and method compromise, selective declassification, harms to individual rights, digital integrity threats, and distortion of public trust. The most serious constraints lie in the absence of sector-specific guidance, the weak integration of consequence testing into the intelligence cycle, and the lack of audit trails capable of verifying disclosure decisions. The proposed CP1 to CP5 auditable disclosure governance model offers a middle path by treating non-classified intelligence dissemination as a problem of legal governance and information policy.



Ultimately, the dissemination of non-classified intelligence cannot be left to institutional communication discretion alone. It requires legal form, written procedure, and an auditable chain of decision-making. That is where openness and secrecy meet as a problem of information governance. Unless the state builds a procedural bridge between consequence testing in the disclosure regime and the protection of intelligence secrets in the intelligence regime, excessive closure will remain the dominant institutional response. The urgent task, therefore, is not only to clarify what must remain secret, but also to establish how non-classified intelligence may be produced, sanitised, disclosed, and reviewed lawfully.

Further research should test the model through case studies of information disputes, stakeholder interviews, and procedural simulations using example nonclassified intelligence products. Such research can also evaluate how the model might operate across different intelligence organisations and how it can be integrated into broader national information security governance.

References:

- Abraham, Rene, Johannes Schneider, and Jan Vom Brocke. "Data Governance: A Conceptual Framework, Structured Review, and Research Agenda." *International Journal of Information Management* 49 (December 2019): 424–38. <https://doi.org/10.1016/j.ijinfomgt.2019.07.008>.
- Badan Intelijen Negara. "Peraturan Badan Intelijen Negara Nomor 1 Tahun 2022 Tentang Organisasi Dan Tata Kerja Badan Intelijen Negara." Republik Indonesia, January 4, 2022.
- Buluc, Ruxandra, Rubén Arcos, and Cristina Ivan. "When Spies Go Public! Lessons Learnt from the Instrumentalization of Intelligence for Strategic Communication in the Run-up to the Russian-Ukrainian War." *Intelligence and National Security* 40, no. 1 (2025): 42–57. <https://doi.org/10.1080/02684527.2024.2405255>.
- Constantino, Jorge, and Ben Wagner. "Accountability and Oversight in the Dutch Intelligence and Security Domains in the Digital Age." *Frontiers in Political Science* 6 (June 2024): 1383026. <https://doi.org/10.3389/fpos.2024.1383026>.
- DalGLISH, Sarah L., Hina Khalid, and Shannon A. McMahon. "Document Analysis in Health Policy Research: The READ Approach." *Health Policy and Planning* 0, no. 0 (2020): 1424–31. <https://doi.org/10.1093/heapol/czaa064>.
- De Werd, Peter. "The Value of Engaged Critique: Civic Intelligence Oversight and the Freedom of Information in the Netherlands." *Intelligence and National Security*, October 22, 2025, 1–26. <https://doi.org/10.1080/02684527.2025.2565938>.
- Díaz-Fernández, Antonio M., and Cristina Del-Real. "Measuring Trust in Intelligence Services: A Conceptual Framework and Exploratory Study." *Democracy and Security* 22, no. 1 (2025): 80–108. <https://doi.org/10.1080/17419166.2025.2459067>.
- Dolata, Mateusz, and Gerhard Schwabe. "Moving beyond Privacy and Airspace Safety: Guidelines for Just Drones in Policing." *Government Information Quarterly* 40, no. 4 (2023): 101874. <https://doi.org/10.1016/j.giq.2023.101874>.
- Dudding, Sasha. "Spinning Secrets: The Dangers of Selective Declassification." *The Yale Law Journal* 130, no. 3 (2021): 708–77.
- Dylan, Huw, and Thomas J. Maguire. "Secret Intelligence and Public Diplomacy in the Ukraine War."



- Survival* 64, no. 4 (2022): 33–74. <https://doi.org/10.1080/00396338.2022.2103257>.
- Fest, Isabelle, Maranke Wieringa, and Ben Wagner. “Paper vs. Practice: How Legal and Ethical Frameworks Influence Public Sector Data Professionals in the Netherlands.” *Patterns* 3, no. 10 (2022): 100604. <https://doi.org/10.1016/j.patter.2022.100604>.
- Juneau, Thomas. “National Security Transparency and Relations with Minority Communities.” *International Journal of Intelligence and CounterIntelligence* 37, no. 1 (2024): 156–74. <https://doi.org/10.1080/08850607.2023.2175630>.
- Komisi Informasi. “Peraturan Komisi Informasi Nomor 1 Tahun 2021 Tentang Standar Layanan Informasi Publik.” Republik Indonesia, June 25, 2021.
- Komisi Informasi Pusat. “Sejarah Komisi Informasi.” Bidang Penelitian dan Dokumentasi Komisi Informasi Pusat, Oktober 2024.
- Lefebvre, Stephane. “State Secrecy: A Literature Review.” *Secrecy and Society* 2, no. 2 (2021). <https://doi.org/10.31979/2377-6188.2021.020209>.
- Marleku, Alfred. “Public Intelligence as a Strategic Tool: The Role of Real-Time Intelligence Disclosure in the Ukraine War.” *Security and Defence Quarterly* 50, no. 2 (2025): 50–65. <https://doi.org/10.35467/sdq/205566>.
- Morgan, Hani. “Conducting a Qualitative Document Analysis.” *The Qualitative Report* 27, no. 1 (2022): 64–77. <https://doi.org/10.46743/2160-3715/2022.5044>.
- Pasek, Judith E. “Defining Information Policy: Relating Issues to the Information Cycle.” *New Review of Academic Librarianship* 21, no. 3 (2015): 286–303. <https://doi.org/10.1080/13614533.2015.1009126>.
- Petersen, Karen Lund. “Three Concepts of Intelligence Communication: Awareness, Advice or Co-Production?” *Intelligence and National Security* 34, no. 3 (2019): 317–28. <https://doi.org/10.1080/02684527.2019.1553371>.
- Republik Indonesia. “Peraturan Pemerintah Nomor 61 Tahun 2010 Tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.” Republik Indonesia, Agustus 2010.
- Republik Indonesia. “Peraturan Presiden Nomor 67 Tahun 2013 Tentang Koordinasi Intelijen Negara.” Republik Indonesia, November 4, 2013.
- Republik Indonesia. “Undang-Undang Nomor 14 Tahun 2018 Tentang Keterbukaan Informasi Publik.” Jakarta, 2018.
- Republik Indonesia. “Undang-Undang Nomor 17 Tahun 2011 Tentang Intelijen Negara.” Jakarta, 2011.
- Ribeiro, Diogo, Vítor Fonte, Luis Felipe Ramos, and João Marco Silva. “Assessing the Information Security Posture of Online Public Services Worldwide: Technical Insights, Trends, and Policy Implications.” *Government Information Quarterly* 42, no. 2 (2025). <https://doi.org/10.1016/j.giq.2025.102031>.
- Sekretariat Jenderal DPR RI. “Naskah Akademik RUU Intelijen Negara Hasil Harmonisasi Baleg.” November 24, 2010.
- Shakoor, Tallat Rønn. “Unwinding the Intelligence Cycle in Denmark.” *International Journal of Intelligence and CounterIntelligence*, April 17, 2023, 1–19. <https://doi.org/10.1080/08850607.2023.2193133>.