

Germany

Germany Establishes an AI Safety and Security Institute

*Maximilian Pralle, Tarmio Frei, Oskar Wernitz, Hannes Bastians and Christoph Winter**

I. Introduction: Virtual Beginnings and Open Questions

On 8 June 2026, Germany formally decided to establish a German AI Safety and Security Institute (DE-AISI).¹ The decision was adopted by the National Security Council and implements Germany's commitment under the 2024 Seoul Declaration's Statement of Intent² to support the development of AI Safety and Security Institutes and to nurture networks between them. It reflects a shift in German AI governance towards strengthening governmental capacity to understand the capabilities, limitations, and security implications of frontier AI models.³ According to the Government, the DE-AISI will provide sci-

entific and technical expertise and support strategic risk assessment.⁴

The initiative draws inspiration from institutions like the UK AI Security Institute (UK AISI), which is regarded as a prominent example of government-backed scientific evaluation of frontier AI models.⁵ Joint statements with the United Kingdom and France indicate that the DE-AISI is intended to become part of the growing international network of AI Safety and Security Institutes.⁶ Government statements also emphasise that the DE-AISI is intended to complement rather than duplicate the governance framework established under the EU AI Act.⁷ In particular, it is expected to support scientific cooperation and frontier AI evaluation with a purely non-reg-

DOI: 10.21552/aire/2026/3/11

* Maximilian Pralle, DPhil candidate in Law, University of Oxford, UK. Dipl. Jur. Tarmio Frei⁰⁰⁰⁹⁻⁰⁰⁰²⁻²¹⁸⁶⁻²⁹⁷², LL.B. and Oskar Wernitz⁰⁰⁰⁹⁻⁰⁰⁰³⁻⁰²⁹³⁻⁷¹⁶³, LL.B., Licencié en Droit, are Summer Research Fellows at the Institute for Law & AI, Cambridge, UK. Dr. Hannes Bastians is a Research Scholar at the Institute for Law & AI. Prof. Christoph Winter is an Assistant Professor of Law and AI, University of Cambridge, the Director of the Cambridge Programme on AI Science & Policy, University of Cambridge, as well as the founding Director of the Institute for Law & AI, Cambridge, UK. For correspondence: <tarmio.frei@law-ai.org>. The authors thank Prof. Dr. Dana Beldiman, M.A., J.D., LL.M. and Dr. André Reinelt for their valuable feedback. The authors are currently conducting research at the Institute for Law & AI on private and public law set-ups for a German AI Safety and Security Institute.

1 Presse- und Informationsamt der Bundesregierung, 'Sitzung des Nationalen Sicherheitsrates im Juni 2026' (*Die Bundesregierung*, 8 June 2026) <<https://www.bundesregierung.de/breg-de/aktuelles/sitzung-des-nationalen-sicherheitsrates-im-juni-2026-2438050>> accessed 18 August 2026. For the formal announcement under the name 'AISi Deutschland', see Bundesministerium für Digitales und Staatsmodernisierung, 'AISi Deutschland gegründet' (Press release 50/2026, 31 August 2026) <<https://bmds.bund.de/aktuelles/pressemitteilungen/detail/aisi-deutschland-gegruendet>> accessed 1 September 2026.

2 'Seoul Statement of Intent toward International Cooperation on AI Safety Science', AI Seoul Summit 2024 (Annex to the Seoul Declaration) (UK Department for Science, Innovation and Technology, 21 May 2024) <<https://www.gov.uk/government/publications/seoul-declaration-for-safe-innovative-and-inclusive-ai-ai-seoul-summit-2024/seoul-statement-of-intent-toward-international-cooperation-on-ai-safety-science-ai-seoul-summit-2024-annex>> accessed 18 August 2026. The Statement of Intent is non-binding.

3 For the necessity of strengthening governmental capabilities regarding frontier AI risks, see Christoph Winter and Charlie

Bullock, 'Radical Optionality: Governing Transformative AI Under Uncertainty' (*Institute for Law & AI*, 23 April 2026) <<https://radical-optionality.ai/>> accessed 18 August 2026.

4 Presse- und Informationsamt der Bundesregierung (n 1).

5 See regarding the reputation of the UK AISI as a renowned AISI: Bundesministerium für Digitales und Staatsmodernisierung, 'Deutschland und Großbritannien vereinbaren Zusammenarbeit bei KI-Sicherheit' (BMDS, 1 July 2026) <<https://bmds.bund.de/aktuelles/pressemitteilungen/detail/deutschland-und-grossbritannien-vereinbaren-zusammenarbeit-bei-ki-sicherheit>> accessed 18 August 2026 ('internationally renowned partner'); Charlie Grossman, 'Making Sense of the UK's AI Security Institute' (*Ada Lovelace Institute*, 13 July 2026) <<https://www.adalovelaceinstitute.org/feature/aisi/>> accessed 18 August 2026. See regarding the DE-AISI's deliberate alignment with leading international institutions: Bundesamt für Sicherheit in der Informationstechnik, 'AISi Deutschland' <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/AISI/aisi_node.html> accessed 1 September 2026.

6 Department for Science, Innovation and Technology, 'United Kingdom-Germany Joint Statement on the Safety and Security of Advanced Artificial Intelligence' (GOV.UK, 30 June 2026) <<https://www.gov.uk/government/publications/uk-germany-joint-statement-on-advanced-ai-safety-and-security/united-kingdom-germany-joint-statement-on-the-safety-and-security-of-advanced-artificial-intelligence>> accessed 18 August 2026. Bundesministerium für Digitales und Staatsmodernisierung, 'Deutschland und Frankreich beschließen engere Zusammenarbeit bei KI und digitaler Souveränität' (Press release 43/2026, 17 July 2026), including the joint statement on AI safety and security <<https://bmds.bund.de/aktuelles/pressemitteilungen/detail/deutschland-und-frankreich-beschliessen-engere-zusammenarbeit-bei-ki-und-digitaler-souveraenitaet>> accessed 14 September 2026.

7 United Kingdom-Germany Joint Statement (n 6), statement by Karsten Wildberger on the EU AI Office's competences.

ulatory mandate distinct from the enforcement functions of the AI Office and the national market surveillance authorities designated under Germany's AI Market Surveillance and Innovation Promotion Act (KI-MIG).⁸

Although the permanent legal structure has yet to be settled, the German Federal Government has indicated that the DE-AISI will initially operate as a virtual institution anchored in a 'nucleus' drawing on existing capacities at the Federal Office for Information Security (BSI – the cybersecurity regulator) and the Federal Network Agency (Bundesnetzagentur, BNetzA).⁹ In this initial build-up phase, the focus will be on security and safety aspects of advanced AI models.¹⁰ In early August 2026, a spokesperson for the Federal Ministry for Digital Transformation and Government Modernisation (BMDS) reportedly confirmed that this nucleus was already operational, describing a step-by-step, modular build-up approach and noting that exchanges with international partner institutions, including counterparts in France and the United Kingdom, and with the AI Office were already under way; the formal announcement of the establishment of the DE-AISI followed on 31 August 2026.¹¹ The subsequent official announcement envisages a broader scope for the long-term mandate but does not fully specify its boundaries.¹²

For the long-term structure of the DE-AISI, current policy proposals advocate for an institution with a narrowly defined technical and scientific mandate, organisational independence, and close integration into Germany's national security architecture, rather than a new regulatory authority.¹³ Several open questions remain, including the exact scope of the DE-AISI's mandate, its financial flexibilities, and its long-term location. This report outlines and comments on each, highlighting the possibility of establishing the DE-AISI as a federally owned limited liability company (GmbH).

II. An AISI with an Unsettled Scope

The most consequential open question concerns the material scope of the DE-AISI's mandate. The National Security Council's decision seems to refer mainly to assessing the cybersecurity-related challenges of advanced AI models for Germany.¹⁴ The nucleus, in turn, is to cover both 'security' (BSI) and 'safety' (BNetzA) aspects of such models.¹⁵ Parliamentary

State Secretary Jarzombek has since indicated a build-up towards an institution positioned more broadly, both thematically and in terms of capacity.¹⁶ The BMDS has confirmed this trajectory, announcing that the DE-AISI will be expanded thematically and in terms of capacity in a second phase.¹⁷ The announcement indicates a broader remit in two further respects. First, the institute is to evaluate not only the risks that advanced AI models present for Germany, but also the opportunities they bring, and to strengthen German resilience in the field of artificial intelligence.¹⁸ Second, the DE-AISI is envisaged to engage beyond the Federal Government and the administration, ensuring a structured transfer of security-relevant findings to business and civil society.¹⁹ A broader design had also been proposed by a group of researchers in October 2025.²⁰ In comparison, the Seoul Statement of Intent frames the role of such in-

8 BGBl. 2026 I Nr. 223. The German AI Market Surveillance and Innovation Promotion Act (KI-MIG) implements the EU AI Act at national level and sets out the national AI Act governance framework.

9 Bundesministerium für Digitales und Staatsmodernisierung (n 1).

10 BT-Drs. 21/7052, 122. See also: Bundesministerium für Digitales und Staatsmodernisierung (n 1).

11 Tim Feldmann et al, 'Trotz Aufbauphase: KI-Sicherheitsinstitut arbeitet schon' (SZ Dossier, 7 August 2026). For the formal announcement on 31 August 2026, see Bundesministerium für Digitales und Staatsmodernisierung (n 1).

12 Bundesministerium für Digitales und Staatsmodernisierung (n 1); BT-Drs. 21/7052, 122.

13 Bitkom, 'Deutsches AI Security Institut (DE-AISI): Positionspapier' (Bitkom, June 2026) <<https://www.bitkom.org/sites/main/files/2026-06/bitkom-positionspapier-deutsches-ai-security-institute.pdf>> accessed 18 August 2026; Philip Fox and Anton Leicht, 'KI-Sicherheit: Warum Deutschland ein AI Security Institute braucht' (Tagesspiegel Background, 17 March 2025) <<https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/warum-deutschland-ein-ai-security-institute-braucht>> accessed 18 August 2026; Monika Schnitzer and Antonia Jülich, 'Deutschland bekommt ein AI Security Institute – jetzt muss es richtig gestaltet werden' *Frankfurter Allgemeine Zeitung* (18 June 2026) <<https://www.faz.net/aktuell/wirtschaft/unternehmen/monika-schnitzer-wie-das-deutsche-ai-security-institute-sein-sollte-accg-200939048.html>> accessed 18 August 2026.

14 Presse- und Informationsamt der Bundesregierung (n 1).

15 BT-Drs. 21/7052, 122.

16 Ibid. This was also echoed by the BMDS, Bundesministerium für Digitales und Staatsmodernisierung (n 1).

17 Bundesministerium für Digitales und Staatsmodernisierung (n 1).

18 Ibid.

19 Ibid.

20 Patrick Schramowski et al, 'Deutsches AI Safety Institut (DAISI): Gründung eines nationalen Instituts zur Gewährleistung sicherer und ethischer Künstlicher Intelligenz' (October 2025) <https://assets.ctfassets.net/jq1xw71av3v5/4uK1tBniQtAGsCC5E7MYP/a4f9156c81b38eb59f026510c401d61e/DAISI_-_Konzeptplan-Okt_2025.pdf> accessed 18 August 2026.

stitutes more narrowly as facilitating ‘AI safety research, testing, and/or developing guidance to advance AI safety for commercially and publicly available AI systems’.²¹

On the distinct question of institutional function, the German policy debate seems to be converging on a non-regulatory, scientific and technical mandate aimed at enabling the Federal Government to reach informed decisions on frontier AI model risks. Interest groups have argued that the DE-AISI should be clearly distinct from regulatory authorities such as the BNetzA and the BSI to enable trust-based cooperation with frontier AI model developers,²² and the BSI itself has recently clarified that the DE-AISI is designed not to carry out regulatory or market surveillance activities.²³ These proposals envision that the DE-AISI would produce recurring cross-departmental situational assessments for the Federal Government, conduct systematic technical evaluations of frontier AI models, carry out research in service of those tasks, contribute to the development of technical standards, and cooperate with partner institutions at national, supranational, and international levels.²⁴ Its focus would extend beyond cybersecurity to chemical, biological, radiological, and nuclear (CBRN) risks and to loss-of-control (LoC) risks,²⁵ comparable to the focus of the UK AISI.²⁶

Another question concerns which models precisely the DE-AISI should observe and evaluate.²⁷ Arguably, a national security-focused institute should not confine itself to general-purpose AI (GPAI) mod-

els with systemic risk within the meaning of the EU AI Act,²⁸ but should also capture more specialised models capable of generating comparable risks: genome language models capable of facilitating the design of dangerous pathogens could be one example.²⁹ The definition should remain technology-neutral, so that the institute’s remit is not restricted only to proprietary models or tied to today’s model architectures. At the same time, defining the frontier of AI capabilities is not straightforward. A functionally wide interpretation of frontier AI could overextend the focus of the DE-AISI.³⁰

Persistent uncertainty about the material scope of the DE-AISI’s mandate will come at a cost. Developers deciding whether to grant pre-deployment access as well as access to otherwise unreleased models need to know whether they are dealing with a scientific partner or with an institution whose remit may later expand into adjacent, potentially regulatory territory. Industry associations have therefore called for a research mandate clearly delineated from that of existing enforcement bodies, arguing that questions of labour law, consumer protection, data protection, and AI ethics are already competently addressed elsewhere.³¹

After all, the preliminary nucleus arrangement may come to sit uneasily with the institute’s intended function. The BNetzA recently became Germany’s central node of the AI Act’s national-level enforcement architecture,³² and the BSI holds its own enforcement powers in the field of information securi-

21 Seoul Statement of Intent toward International Cooperation on AI Safety Science (n 2).

22 Fox and Leicht (n 13); Bitkom (n 13); Schnitzer and Jülich (n 13).

23 Bundesamt für Sicherheit in der Informationstechnik (n 5).

24 See, eg: Bitkom (n 13). This aligns mostly with the description by the BSI itself, Bundesamt für Sicherheit in der Informationstechnik (n 5).

25 Bitkom (n 13), 2, proposes coverage of CBRN, loss-of-control, and mass manipulation risks. The BMDS announcement expressly identifies cybersecurity and loss-of-control risks, but does not expressly mention CBRN risks: Bundesministerium für Digitales und Staatsmodernisierung (n 1).

26 Grossman (n 5).

27 Official statements use both model and system terminology: the BMDS mainly lists advanced AI models (Bundesministerium für Digitales und Staatsmodernisierung (n 1)), while the BSI describes the DE-AISI as an evaluation body for capable AI systems while listing the technical evaluation of AI models among its core tasks (Bundesamt für Sicherheit in der Informationstechnik (n 5)). Evaluating AI systems could create practical overlap with the work of market surveillance authorities under the KI-MIG.

28 See art 51 AI Act. For more details: Gregor Gindlin, ‘Article 51: Classification of general-purpose AI models as general-purpose AI

models with systemic risk’ (*Cambridge Commentary on EU General-Purpose AI Law*, 21 July 2026) <<https://cambridge-commentary.ai/article-51/>> accessed 18 August 2026.

29 Such an approach would allow the DE-AISI to correct for potential under-inclusivity in the criteria for the classification of general-purpose AI models with systemic risk under art 51 of the AI Act. On governance misspecification generally, see Christoph Winter and Charlie Bullock, ‘The Governance Misspecification Problem’ (LawAI Working Paper No. 3-2024, 2024) <<https://law-ai.org/wp-content/uploads/2024/10/Governance-misspecification-1.pdf>> accessed 18 August 2026. Regarding AI-generated bacteriophages, see Samuel H King et al, ‘Generative Design of Bacteriophages with Genome Language Models’ (2026) 393 Science eaec2657. Recital 102 of the recently proposed European Biotech Act explicitly highlights that AI models in biological applications may pose ‘biological systemic risks’ even if they do not classify as general-purpose AI models (with systemic risks) under the AI Act, COM(2025) 1022 final.

30 See regarding the difficulties of defining frontier models: Charlie Bullock et al, ‘Legal Considerations for Defining “Frontier Model”’ (LawAI Working Paper No. 2-2024, 2024) <<https://law-ai.org/wp-content/uploads/2024/09/Legal-Considerations-for-Defining-Frontier-Model.pdf>> accessed 18 August 2026..

31 Fox and Leicht (n 13); Bitkom (n 13); Schnitzer and Jülich (n 13).

32 See § 2(1) KI-MIG.

ty.³³ An institute housed within or governed by authorities exercising such powers may struggle to obtain the confidential access on which its work depends. For instance, GPAI model providers may worry that the BNetzA could use information voluntarily shared with the DE-AISI to request the European Commission to exercise its powers to enforce Chapter V of the AI Act, where this is necessary and proportionate to assist the BNetzA in fulfilling its market surveillance tasks.³⁴ Closing precisely this kind of access gap is among the institute's purposes and of outsized importance to national security. Indeed, obtaining pre-release access to frontier models may prove difficult in any event as recent reporting on the UK AI Security Institute illustrates.³⁵ Whatever its institutional set-up ends up being, it may therefore be advisable to ensure a sufficiently clear delineation between the DE-AISI and regulatory powers. This may mean limiting the cooperation between the DE-AISI and the BSI and the BNetzA to general, non-developer-specific findings on frontier AI risks, rather than confidential information capable of being used for regulatory purposes. In this respect, it is promising that the BSI has expressly described the DE-AISI as a non-regulatory institution.³⁶

III. Pay, Flexibility, and the Case for a GmbH

Germany's Federal Digital Minister has stated that the DE-AISI should be staffed with 'top expertise

from world-class experts'.³⁷ Delivering on that ambition will be difficult within ordinary German public-sector pay structures, which may be insufficient to compete for highly sought-after frontier AI experts. One industry report by the payroll platform Rise records a 45% increase in compensation for AI safety and alignment specialists since 2023.³⁸ The UK AISI has recognised these dynamics. It operates not only with GBP 66 million in annual funding and priority access to compute, but also with a more competitive salary structure than the rest of the civil service.³⁹ Proposals in the German debate have mostly suggested funding similar to that of the UK institute ranging from EUR 60 million⁴⁰ to at least EUR 75 million annually.⁴¹

However, funding levels alone do not determine whether these resources can be deployed effectively. Choosing a legal form that allows the DE-AISI to effectively deploy funding will be equally crucial. Establishing the institute as a federally owned GmbH would be a promising option in this regard. It would constitute a formal privatisation (formelle Privatisierung), leaving the operational task itself in state hands while changing only the organisational vehicle through which it is performed.⁴² A reference point for formal privatisation of this kind is the Federal Agency for Disruptive Innovation (Bundesagentur für Sprunginnovationen, SPRIND).⁴³ SPRIND is a wholly federally owned GmbH created to fund high-risk innovation projects and governed by its own statute, the SPRIND Act (SPRIND-Freiheitsgesetz⁴⁴) of 2023.⁴⁵ It was designed for a field in which recruit-

33 See § 3 BSIG (Act on the Federal Office for Information Security).

34 Art 88(2) AI Act permits market surveillance authorities to request the Commission to exercise its powers where necessary and proportionate to assist with their tasks under the Act.

35 Lucy Fisher and Madhumita Murgia, 'Anthropic Withheld Latest AI Model from UK Testing Agency' *Financial Times* (9 September 2026) <<https://www.ft.com/content/560e1c8b-f163-4fd6-b604-e905550ac870>> accessed 10 September 2026.

36 Bundesamt für Sicherheit in der Informationstechnik (n 5).

37 'Künstliche Intelligenz: Bund plant KI-Sicherheitsinstitut für bessere Risikoanalyse' *Tagesspiegel* (9 June 2026) <<https://www.tagesspiegel.de/gesellschaft/medien/kunstliche-intelligenz-bund-plant-ki-sicherheitsinstitut-fur-bessere-risikoanalyse-15694282.html>> accessed 18 August 2026 ('Top-Expertise von Experten auf Weltniveau'; authors' translation).

38 Rise, 'AI Talent Salary Report 2026' (10 February 2026) <<https://www.riseworks.io/blog/ai-talent-salary-report-2025>> accessed 14 September 2026.

39 AI Security Institute, 'About' <<https://www.aisi.gov.uk/about/>> and 'Careers' <<https://www.aisi.gov.uk/careers/>> accessed 14 September 2026.

ber 2026; Grossman (n 5). The careers page describes a technical talent allowance. For another example, the Italian National Cybersecurity Agency (ACN) links the treatment of its permanent staff to that of Bank of Italy staff with equivalent functions and responsibilities: Decreto-legge 14 giugno 2021, n. 82, art 12(1)(a), GU Serie Generale n. 140, 14 June 2021, as converted by Legge 4 agosto 2021, n. 109, GU Serie Generale n. 185, 4 August 2021.

40 Fox and Leicht (n 13).

41 Bitkom (n 13), 2, 4, proposes at least EUR 100 million for the first two years and subsequently at least EUR 75 million annually.

42 Formal privatisation, also referred to as organisational privatisation, denotes the process by which the state adopts a private-law organisational form for the performance of a public task without relinquishing responsibility for that task, see eg Hubertus Gersdorf, 'Privatisierung öffentlicher Aufgaben — Gestaltungsmöglichkeiten, Grenzen, Regelungsbedarf' (2008) 63(17) JZ 831 (831–832).

43 Fox and Leicht (n 13); Bitkom (n 13).

44 BGBl. 2023 I Nr. 415.

45 See the official website: <<https://www.sprind.org/>> accessed 18 August 2026.

ment and funding decisions must be taken quickly and in competition with the private sector. In several ways, the DE-AISI faces a comparable situation, necessitating a legal form that allows it to meet similar key challenges.

One particular challenge is the DE-AISI's staffing. As a company under private law, the institute would not be bound by public-sector collective agreements in the same way as a federal authority. It could seek exemptions from the prohibition on preferential treatment (*Besserstellungsverbot*), which otherwise prevents federally funded bodies from paying their staff more than comparable federal employees. § 5 of the SPRIND Act transfers that decision to the company itself where compelling reasons so require, based on the legislature's reasoning that contract negotiations in highly competitive fields must be conducted quickly and concluded with binding effect. Bitkom, one of Germany's largest digital industry associations, has argued for a comparable arrangement for the DE-AISI.⁴⁶

As for budgetary flexibility, the frontier AI risk landscape develops on timelines that do not align with annual budget tranches. Evaluation and research priorities in this field can shift within months, if not weeks. § 15(2) of the Federal Budget Code (*Bunde-*

shaushaltsordnung) permits appropriations to be designated for self-administration (*Selbstbewirtschaftung*), allowing funds to be carried across financial years and redeployed within the approved purposes as project needs change. § 3(2) of the SPRIND Act makes use of this instrument for 30% of the annual federal allocation to the company. The same instrument has been extended to non-university research institutions to strengthen their performance and international competitiveness,⁴⁷ which suggests its relevance for a body operating in a field that is at once fast-moving and research-based, such as the DE-AISI.

Regarding governance, the articles of association (*Gesellschaftsvertrag*) would allow the Federal Government's specific requirements to be reflected in tailored form,⁴⁸ while limited liability, in principle, caps the exposure of the federal budget.⁴⁹ Democratic accountability can be maintained through the instruments of company law. The Federal Government, as sole shareholder, would appoint the executive director, could issue instructions, and would hold comprehensive information rights.⁵⁰ Furthermore, the GmbH structure allows for a high degree of organisational and personnel flexibility.⁵¹

None of this follows necessarily from the choice of the GmbH as the legal form as such. As in the case of SPRIND, it depends on the enabling legislation providing for it.⁵² In particular, it depends on exemptions from the prohibition on preferential treatment and on the self-administration rate adopted, as well as on the articles of association. Whether comparable arrangements could be achieved within a public law structure remains an open question. In its July 2026 parliamentary response, the Federal Government stated that it was not yet in a position to provide details on the institute's long-term legal structure.⁵³

IV. A Location Fit for Purpose

The Federal Government initially deferred a decision on the DE-AISI's location. On 31 August 2026, it announced that the institute would be established in Berlin, where the virtual nucleus formed by the BSI and the BNetzA now operates.⁵⁴ Reports suggest the choice of location for this first phase of the DE-AISI was driven by the aim of securing close proximity to the work of the Federal Government; the BMDS, the Federal Ministry of the Interior and the Chancellery

46 Bitkom (n 13), 3.

47 Henning Tappe, '§ 15 BHO' in Christoph Gröpl (ed), *BHO/LHO* (2nd edn, CH Beck 2019) para 40.

48 See Martin Burgi, '§ 10 Entwicklungslinien' in Dirk Ehlers and Hermann Pünder (eds), *Allgemeines Verwaltungsrecht* (16th edn, CF Müller 2022) para 15; Eberhard Schmidt-Aßmann, *Das allgemeine Verwaltungsrecht als Ordnungsidee* (2nd edn, Springer 2004) ch 5, para 51.

49 See Christoph Brüning, '§ 5 Öffentliche Unternehmen im Wettbewerbs- und Vergaberecht' in Martin Schulte and Joachim Kloos (eds), *Handbuch Öffentliches Wirtschaftsrecht* (1st edn, CH Beck 2016) para 22; Christoph Teichmann, '§ 25 Umsetzung der verwaltungsrechtlichen Vorgaben betreffend das Öffentliche Unternehmen im Gesellschaftsrecht' in Martin Burgi and Mathias Habersack (eds), *Handbuch Öffentliches Recht des Unternehmens* (1st edn, CH Beck 2023) para 42; Andreas Voßkuhle and Jakob Schemmel, 'Grundwissen – Öffentliches Recht: Privatisierung' (2023) JuS 725 (726).

50 See Teichmann (n 49) paras 84, 86, 114, 141.

51 See Nikolaus Müller, *Rechtsformenwahl bei der Erfüllung öffentlicher Aufgaben* (Carl Heymanns 1993) 405.

52 Enabling legislation would be constitutionally required for the establishment of the DE-AISI in any case. This, according to the authors, follows from art 87(3) Grundgesetz, see Christoph Winter et al, 'Ein KI-Sicherheitsinstitut für Deutschland: Grundfragen zur verfassungs- und verwaltungsrechtlichen Zulässigkeit des GmbH-Modells', KIR 2026 (forthcoming).

53 BT-Drs. 21/7052, 122.

54 Bundesministerium für Digitales und Staatsmodernisierung (n 1).

were all involved in the decision.⁵⁵ Where the institute will be sited in its second phase, however, appears to remain undecided.

Both the Saarland and Bavaria had formally campaigned for the institute. In August 2026, the CDU group in the Saarland state parliament – in opposition at state level, but the party of the Chancellor and, with its sister party the CSU, of the ministries leading on the DE-AISI – formally called for the institute to be based in Saarbrücken. Stephan Toscani, chair of the group, described the Saarland as ‘the ideal location’.⁵⁶ Saarbrücken hosts Saarland University, the German Research Center for Artificial Intelligence (DFKI), the CISPA Helmholtz Center for Information Security, two Max Planck Institutes, as well as branch offices of both the BSI and the BNetzA.⁵⁷ Minister-President Anke Rehlinger offered financial support, including the possibility of temporarily covering the institute’s rent, and several Saarland research institutions backed the bid in a letter.⁵⁸ Bavaria campaigned for Munich,⁵⁹ individual members of the Bundestag advocated for Dresden⁶⁰ and Darmstadt.⁶¹ Bonn, for its part, would have placed the DE-AISI at the same location as the BSI headquarters.⁶² Following the decision on the institute’s structure and location for its first phase, the Saarland’s Minister of Economy, Innovation, Digital Affairs, and Energy stated that he would have preferred a single decision on the institute as a whole, taken strictly on substan-

tive criteria, and that the state would pursue its chance in the second phase.⁶³

The Berlin location aligns with the institute’s intended advisory function. If the DE-AISI’s defining task will be advising the Federal Government on frontier AI risks, its work will consist largely of recurring cross-departmental situational assessments, ad hoc analysis when risks shift at short notice, and exchanges that might involve classified material. In this respect, proximity to the ministries carries particular weight, as the UK AISI’s location in London illustrates. The relocation of the headquarters of the Federal Intelligence Service (BND) from Pullach to Berlin was justified on similar grounds, given the need for swift communication and intensive coordination between the BND and federal government bodies.⁶⁴ Berlin also offers access to one of Germany’s largest AI industry clusters, hosts a DFKI branch,⁶⁵ and, as a capital city, may prove easier to recruit for than the alternatives.

Regional policy considerations pull in the other direction and are likely to resurface in the second phase. Germany has a long-standing practice of distributing federal institutions across the country, and the Saarland bid is expressly framed as part of that state’s structural transition towards a technology location.⁶⁶ These are legitimate objectives in their own right, but they are distinct from the question of where the institute can most effectively perform its advisory func-

55 ‘Bundesregierung siedelt KI-Sicherheitsinstitut in Berlin an’ *City-News* (September 2026) <<https://www.city-news.de/bundesregierung-siedelt-ki-sicherheitsinstitut-in-berlin-an/253038/>> accessed 7 September 2026.

56 ‘CDU will nationales KI-Sicherheitsinstitut ins Saarland holen’ *Homburg1* (5 August 2026) <<https://homburg1.de/cdu-will-nationales-ki-sicherheitsinstitut-ins-saarland-holen-256028/>> accessed 18 August 2026, translated from German.

57 Ibid.

58 ‘Saarland hält Saarbrücken als Standort für KI-Sicherheitsinstitut im Rennen’ *Homburg1* (3 September 2026) <<https://homburg1.de/saarland-haelt-saarbruecken-als-standort-fuer-ki-sicherheitsinstitut-im-rennen-260008/>> accessed 8 September 2026.

59 Bavarian State Government, ‘Dr. Mehring will KI-Sicherheitsinstitut des Bundes nach Bayern holen: Bayerns Digitalminister wirbt in Berlin für München als Standort’ (21 August 2026) <<https://www.bayern.de/dr-mehring-will-ki-sicherheitsinstitut-des-bundes-nach-bayern-holen-bayerns-digitalminister-wirbt-in-berlin-fuer-muenchen-als-standort/>> accessed 14 September 2026.

60 Markus Reichel, ‘Geplantes KI-Sicherheitsinstitut: Dresden gehört in die Standortdebatte’ (28 August 2026) <<https://www.markus-reichel.de/aktuelles/2026/wochenrueckblick-24-28-08-2026/>> accessed 8 September 2026.

61 Thomas Pauls, ‘Darmstadt bietet ideale Voraussetzungen für das zu gründende Nationale KI-Sicherheitsinstitut’ (19 August 2026)

<<https://www.thomas-pauls.de/aktuelles/202608kisicherheitsinstitut/>> accessed 8 September 2026.

62 The main location of the BSI is Bonn, see BSI, ‘Standorte des BSI’ <https://www.bsi.bund.de/DE/Das-BSI/BSI-Standorte/bsi-standorte_node.html> accessed 18 August 2026.

63 Saarländischer Rundfunk, ‘KI-Sicherheitszentrum kommt zunächst nicht ins Saarland, trotzdem besteht noch Hoffnung’ (1 September 2026) <https://www.sr.de/sr/home/nachrichten/politik_wirtschaft/ki_sicherheitszentrum_kommt_nicht_ins_saarland_100.html> accessed 15 September 2026.

64 BT-Drs. 14/3499, 1; ‘Aus für Pullach: BND zieht nach Berlin’ (*Der Spiegel*, 11 April 2003) <<https://www.spiegel.de/politik/deutschland/aus-fuer-pullach-bnd-zieht-nach-berlin-a-244513.html>> accessed 18 August 2026. See also BND, ‘Unsere Standorte’ <https://www.bnd.bund.de/DE/Der_BND/Unsere-Standorte/standorte-node.html> accessed 19 August 2026. The BND itself describes proximity to the government in Berlin as being as decisive for its work as a worldwide presence.

65 Cf AppliedAI Institute for Europe, ‘KI-Startup Landscape (2025) Die achte jährliche KI-Startup Landscape’ <<https://www.appliedai-institute.de/publikationen/ki-startup-landscape-2025/>> accessed 18 August 2026. See also DFKI, ‘DFKI Labor Berlin’ <<https://www.dfk.de/web/ueber-uns/standorte-kontakt/berlin/>> accessed 14 September 2026.

66 ‘CDU will nationales KI-Sicherheitsinstitut ins Saarland holen’ (n 56).

tion. Insofar as the above considerations of proximity to the Federal Government and talent recruitment are crucial factors, they point towards Berlin for the second phase as well.

V. Conclusion: What Germany Stands to Gain, or Forgo

The establishment of the DE-AISI is an important opportunity for Germany to contribute to the safety and security of frontier AI models as their risks for national security and critical infrastructure become increasingly central. Existing institutes provide case studies for success factors and possible failure modes. For example, the UK AI Security Institute has benefited from financial flexibility in hiring, access to compute, an attractive location, and a scientific mandate clearly distinct from regulatory functions – a feature now expressly included in the German institute’s published design. Drawing on these experiences, the DE-AISI can make vital contributions to national security by assessing frontier AI risks specifically in line with the mandate of the German National Security Council.

Such a role provides a rationale for dedicated national capacity alongside EU-level and international cooperation. National security remains the responsi-

bility of each Member State, while the AI Office supervises general-purpose AI model obligations at Union level. The AI Act’s definition of systemic risk refers to a significant impact on the Union market and harms that can propagate at scale across the value chain rather than to the exposure of any single Member State.⁶⁷

Until these capacities are fully built up, Germany’s ability to anticipate and respond to frontier AI risks remains substantially dependent on what partner institutions abroad are willing to share. Timely progress will therefore be essential. The decision to establish the institute came more than two years after Germany endorsed the Seoul Statement of Intent in May 2024.⁶⁸

Two important elements of the institutional design have now been clarified. Berlin has been confirmed as the seat of the first phase, securing the proximity to the Federal Government that the institute’s advisory work requires. Whether the second-phase expansion will involve a separate location remains open. What is more, the institute’s non-regulatory character has been stated expressly. The legal form, by contrast, remains undecided. A GmbH could afford the needed financial and personnel flexibilities, subject to appropriate statutory and budgetary arrangements that clearly define the institute’s mandate and its relation to other governmental bodies.

If these steps are taken, the DE-AISI can move to the forefront of international AI safety and security institutions and anchor Germany’s preparedness for frontier AI risks.

⁶⁷ Art 4(2) TEU; arts 2(3), 3(65), and 88(1) AI Act.

⁶⁸ Seoul Statement of Intent (n 2), 21 May 2024; Presse- und Informationsamt der Bundesregierung (n 1), 8 June 2026.