LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/3104

A20, A09

CYBER|NTELLIGENCE
.Institute

cyberintelligence.institute // Friedrich-Ebert-Anlage 49 // 60308 Frankfurt a.M.

Herrn
André Kuper MdL
Präsident des Landtags NRW
Platz des Landtags 1
40221 Düsseldorf

cyberintelligence.institute GmbH
MesseTurm // Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.

Dr. Michael Littger, LL.M.oec.
Europajurist
Strategy Director // Mitglied der Geschäftsleitung
Michael.Littger@cyberintelligence.institute

Per E-Mail: anhoerung@landtag.nrw.de

Frankfurt a.M., 29.10.2025

Betreff: **Schriftliche Stellungnahme zum Gesetz zur Stärkung der Informationssicherheit des Landes Nordrhein-Westfalen (Informationssicherheitsgesetz Nordrhein-Westfalen – InfoSiG NRW) Gesetzentwurf der Landesregierung, Drucksache 18/14581**

Berufener Sachverständiger:
Dr. Michael Littger, Strategiedirektor cyberintelligence.institute

Sehr geehrter Herr Präsident,

ich bedanke mich für die Möglichkeit zur fachlichen Stellungnahme des benannten Gesetzes im Rahmen der nachfolgenden Ausführungen:

Allgemeine Anmerkungen

Die allgegenwärtige Gefahr von sicherheitsrelevanten Vorfällen in der öffentlichen Verwaltung mit potenziell erheblichen Auswirkungen auf ihre Leistungsfähigkeit und Bereitstellung auch grundlegender Dienste für die Bevölkerung und Wirtschaft erfordert eine mutige und zügige Verbesserung einer ganzheitlich gedachten IT-Sicherheit.

Die übergeordnete **Zielsetzung des Informationssicherheitsgesetz NRW**, die Vorgaben der NIS-2 Richtlinie für das Bundesland NRW umzusetzen und dabei teilweise auch über die gesetzlichen Mindestanforderungen zu gehen, wird **uneingeschränkt befürwortet** und kann auch als Vorbild für weitere Bundesländer gewertet werden.

An dieser Stelle ist zu begrüßen, dass das InfoSiG NRW einen **gefahrübergreifenden Ansatz** verfolgt, der angesichts der vielfältigen Formen und Ursachen gegenwärtiger Beeinträchtigungen der IT-Sicherheit für eine angemessene Flexibilität von Abwehr- und Schutzmaßnahmen erforderlich ist.

Es sollte jedoch geprüft werden, inwieweit die Aufrechterhaltung auch von Verwaltungsdiensten für den Fall gewährleistet wird, dass getroffene Sicherheitsmaßnahmen nach diesem Gesetz nicht ausreichen, um jederzeit wenigstens einen Notbetrieb aufrechtzuerhalten (**Business Continuity Management**).

Spezielle Anmerkungen

§ 2 – Geltungsbereich

1) Zum Geltungsbereich des Gesetzes in § 2 ist eine explizite **Erweiterung auf den Landtag NRW geboten** als notwendige **Rechtsgrundlage** für einhergehende Befugnisse, Sicherheitslücken, Schadprogrammen sowie Angriffe auf das Landtagsnetz zu identifizieren, die unabhängig von der Anbindung an das Landesverwaltungsnetz nach § 2 Abs. 1 Nr. 2 erfolgen sollen.

   Mit der Erweiterung des Anwendungsbereich auf den Landtag müsste der Landtag durch Beschluss ergänzend eine **Informationssicherheitsleitlinie** festlegen, die für ihn, seine Gremien, seine Mitglieder und deren Beschäftigte, seine Fraktionen und deren Beschäftigte sowie für die Landtagsverwaltung gelten und **nach deren Maßgabe die §§ 4 bis 18** des InfoSiG NRW entsprechend anzuwenden sind.

   Wegen der Details dieser Informationssicherheitsleitlinie nehme ich Bezug auf den Vorschlag 2 der Ergebnisse des „Gutachtens zur Rechtmäßigkeit des Einsatzes von Angriffserkennung im Landtagsnetz“ durch das CII im Auftrag des Landtages NRW vom Oktober 2025.

2) Das Gesetz sieht davon ab, den **Geltungsbereich auf Gemeinden zu erweitern**, was dem Land nach Art. 2. Abs. 5 NIS-2-RL möglich wäre. Damit wird eine **Chance vertan**, das Sicherheitsniveau in der gesamtstaatlichen Struktur auf ein höheres Niveau zu heben. Soweit die Entscheidung aus praktischen Erwägungen der kommunalen Fähigkeiten und Ressourcen erfolgte, können diese nicht überzeugen, da mit dem Gesetz entsprechende Unterstützerstrukturen geschaffen werden könnten.

   In jedem Fall ist eine Klarstellung im Umgang mit der unteren Landesebene zu empfehlen, die im kommunalen Vollzug tätig werden und damit praktisch unter den aktuell vorgesehenen Anwendungsbereich fallen. Hier sollte das Gesetz einen Hinweis auf das **Erfordernis spezieller Abstimmungs- und Unterstützungsbedarfe** aufnehmen.

§ 3 – Begriffe

Die Definition der Rechtsbegriffe ist teilweise nicht hinreichend klar, teilweise zu eng, teilweise zu breit gefasst:

1) **Cyberbedrohungen** I Die Definition beschränkt sich auf Vorfälle in IT-Systemen, die Personen schädigen könnten. Hier ist zu empfehlen, dass auch mögliche Sachschäden als konstituierende Folge einbezogen werden, die keine oder nur mittelbare Schädigung von Personen verursachen können.

2) **Erhebliche Cyberbedrohung** I Die Definition erfordert nach dem InfoSiG NRW eine „doppelte Erheblichkeit“ der Bedrohung, nämlich in Bezug auf die IT-Beeinträchtigung als auch auf die Schadensfolge. Hier sollte es genügen, wenn bereits *einer der beiden Bedrohungen* erheblich ist. Damit fallen z.B. auch geringfügige IT-Beeinträchtigungen unter den Begriff, wenn diese erhebliche Schäden bewirken können – und umgekehrt.

§ 4 bis § 6 – Zuständigkeiten und CSIRT

Die Zuständigkeit für die Informationssicherheit in der Landesverwaltung ordnet das Gesetz dem Digitalministerium des Landes zu. Diese Zuordnung könnte zunächst überraschen, als Cybersicherheit grundsätzlich bei dem Innenministerium liegt. Tatsächlich aber rechtfertigt die Sachnähe zu Digitalisierungsfragen der Verwaltung diese Zuständigkeit, die damit auch spiegelbildlich zur Zuständigkeit des Digitalministeriums auf Bundesebene ist.

Die **Aufwertung der Stabsstelle des CISO** innerhalb des Digitalministeriums zur „zuständigen Stelle“ im Sinne der NIS-2 ist zu **befürworten** sowie auch deren operative Unterstützung des Computer-Notfallteams bei IT.NRW. Insbesondere werden auf diese Weise Synergien anstelle neuer Einrichtungen geschaffen.

§ 7 – Identifizierung wichtiger Behörden

Die Identifizierung „wichtiger Behörden“ in § 7 ist konstitutionell u.a. für die entsprechenden Verpflichtungen zu Risikomanagement-Maßnahmen. Ihr kommt daher eine enorme Bedeutung zu, die zutreffenderweise den Ministerpräsidenten bzw. den zuständigen Ministerien obliegen soll.

Zur Umsetzung verweisen die Erläuterungen des Gesetzes auf das Identifizierungskonzept des IT-Planungsrats, das den Kriterien der Bestimmtheit hinreichend genügt.

§ 8 – Risikomanagementmaßnahmen

Die Regelungen zu den Risikomanagementmaßnahmen orientieren sich im Wesentlichen an den Vorgaben des NIS2. **Positiv** ist hierbei, dass sich das InfoSiG NRW hierbei verstärkt am **Gefahrenansatz ausgerichtet** sowie auch dem **Risiko der digitalen Lieferketten** einen besonderen Stellenwert einräumen.

In diesem Kontext ist zu empfehlen, einen ausdrücklichen Passus aufzunehmen, wonach **digitalsouveräne Diensten und Technologien**, die nur dem Rechtsregime der EU unterworfen sind, grundsätzlich zu bevorzugen sind, um Abhängigkeiten und Unwägbarkeiten in der öffentlichen Verwaltung auch mit Blick auf geopolitische Risiken zu reduzieren.

Sehr zu **begrüßen** ist, dass das Gesetz in seinen Erläuterungen ausdrücklichen **Bezug auf den BSI-Grundschutzstandard** nimmt. Darüber sollte ein Hinweis in den Erläuterungen aufgenommen werden, dass die Beachtung von BSI-Grundschutzvorgaben auf Landesebene eine Nachahmung durch Kommunen aktiv befördern soll.

§ 9 Berichtspflichten

Der **Katalog der Berichts- und Meldepflichten** für wichtige Behörden sollten auf Beinahe-Vorfälle, Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle **erweitert** werden. Zudem sollten sonstige Gefährdungen wie **Sabotage oder Desinformation** in den Meldekatalog aufgenommen werden.

Es sollte in den Gesetzestext aufgenommen werden, dass Meldungen **ausschließlich zur Verbesserung der Informationssicherheit** verwendet werden dürfen und eine Weitergabe der Informationen zur Ausnutzung gemeldeter Sicherheitslücken nicht stattfindet.

§11 – Empfehlungen durch das Digitalministerium

Die Kompetenz des Digitalministeriums zur **Empfehlung konkreter Produkte**, Dienste und Prozesse sowie auch dezidierter Normen bezweckt die einheitliche Anwendung von § 8 InfoSiG NRW, die durch weitergehende Befugnisse der zuständigen Behörde im weiteren Verfahren auch verbindlich angeordnet werden können.

Dieser Ansatz spiegelt den Ansatz auf Bundesebene, dass die Kompetenz für IT-Sicherheit in der Verwaltung über Gestaltungsoptionen für eine einheitliche Umsetzung gegenüber Behörden anderer Ressorts bekräftigt werden. Dieser **Ansatz ist zu begrüßen** und aufgrund des Mittels der „Empfehlungen“ auch **im Grundsatz** auch **verhältnismäßig**.

§12 – Aufsichts- und Durchsetzungsmaßnahmen

Die Regelungen der Aufsichts- und Durchsetzungsmaßnahmen ist grundsätzlich durch die Vorschrift des Art. 33 Abs. 2 NIS-2-RL gedeckt, jedoch überrascht, dass keinerlei Leitplanken für die Benennung der „erforderlichen“ Maßnahmen vorgegeben werden. Rechtstechnisch ist zu empfehlen, jedenfalls in den Erwägungen des Gesetzes einen **Rückbezug auf den Umfang in Art. 33 Abs. 2 NIS-2-RL** zu nehmen, um einer Ausuferung entgegenzuwirken.

§ 15 bis 17 Datenerhebung

Zu begrüßen sind die umfänglichen Regelungen der § 15 ff. InfoSiG NRW, welche die datenschutzrechtlichen Befugnissen und Vorkehrungen zur sicheren Verarbeitung personenbezogenen Daten insbesondere der zuständigen Behörden nun insgesamt auf **ausgewogene Weise** konkretisieren.

Frankfurt am Main / Berlin, 29.10.2025

Dr. Michael Littger
CII-Strategiedirektor