

KONINKRIJK BELGIË

ROYAUME DE BELGIQUE

Federaal Agentschap voor Nucleaire
Controle

Agence fédérale de Contrôle nucléaire

Koninklijk besluit tot uitvoering van artikel 17sexies, §1, van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

Arrêté royal portant exécution de l'article 17sexies, §1, de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen
zullen, Onze Groet.

Philippe, Roi des Belges,
A tous, présents et à venir, Salut.

Gelet op de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, artikel 17sexies, §1, ingevoegd bij wet van 5 april 2019 en artikel 24bis ingevoegd bij wet van 7 mei 2017;

Vu la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, l'article 17sexies, §1, inséré par la loi du 5 avril 2019, et l'article 24bis, inséré par la loi du 7 mai 2017 ;

Gelet op het advies van het Centrum voor Cybersecurity België van 27 februari 2025;

Vu l'avis du Centre pour la Cybersécurité Belgique du 27 février 2025 ;

Gelet op het voorstel van het Federaal Agentschap voor Nucleaire Controle verstuurd aan de Minister van Veiligheid en Binnenlandse Zaken op 10/12/2025;

Vu la proposition de l'Agence fédérale de Contrôle nucléaire envoyée au Ministre de la Sécurité et de l'Intérieur le 10/12/2025 ;

Gelet op het advies XX van de Raad van State, gegeven op XX/XX/2025, met toepassing van artikel 84, §1, eerste lid, 1°, van de op 12 januari 1973 gecoördineerde wetten op de Raad van State;

Vu l'avis XX du Conseil d'Etat, donné le XX/XX/2025, en application de l'article 84, § 1, alinéa 1, 1°, des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973 ;

Overwegende dat de bepalingen van de wet van 15 april 1994 die het wettelijk kader voor nucleaire cyberbeveiliging vastleggen, in werking zijn getreden door het koninklijk besluit van 30 juni 2024 betreffende de inwerkingtreding van de wet van 5 april 2019 houdende wijziging van de wet van 15 april

Considérant que les dispositions de la loi du 15 avril 1994 qui tracent le cadre légal de la cybersécurité nucléaire ont été mises en vigueur par l'arrêté royal du 30 juin 2024 relatif à la mise en vigueur de la loi du 5 avril 2019 portant modification de la loi du 15 avril 1994 relative à la protection de la population

1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle betreffende de nucleaire cyberbeveiliging en houdende aanduiding van de autoriteiten bedoeld in artikel 17sexies, §1, §2, en §4, van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle; overwegende dat dit zelfde koninklijk besluit van 30 juni 2024 de overheden aanwijst die, naast het Federaal Agentschap voor Nucleaire Controle, zullen worden betrokken bij het opstellen van de verschillende maatregelen of het uitvoeren van bepaalde taken;

Overwegende dat de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid niet van toepassing is op de klasse I inrichtingen overeenkomstig de bepalingen van zijn artikel 5, §4, 8°), lid 2, van dezelfde wet ;

Op de voordracht van de Minister van Veiligheid en Binnenlandse Zaken;

Hebben Wij besloten en besluiten Wij:

et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire concernant la cybersécurité nucléaire et désignant les autorités visées à l'article 17sexies, §1, §2 et §4, de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire ; considérant que ce même arrêté royal du 30 juin 2024 désigne les autorités qui seront associées, aux côtés de l'Agence fédérale de Contrôle nucléaire, à la confection des diverses mesures ou à l'accomplissement de certaines tâches ;

Considérant que la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique n'est pas d'application aux établissements de classe I selon les modalités de son article 5, §4, 8°), alinéa 2 ;

Sur la proposition de Notre Ministre de la Sécurité et de l'Intérieur;

Nous avons arrêté et arrêtons :

Hoofdstuk I: Algemene bepalingen

Artikel 1. Definities

§1. Tenzij anders bepaald in §2, gelden voor de toepassing van dit besluit de definities die gegeven zijn in artikel 1 en 1bis van de Wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle en in artikel 2 van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de

Chapitre I : Dispositions générales

Article 1. Définitions

§1. Sauf autrement déterminé au §2, pour l'application du présent arrêté, les définitions données aux articles 1 et 1bis de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire et à l'article 2 de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants s'appliquent.

werknemers en van het leefmilieu tegen het gevaar van de ioniserende stralingen;

§2. Voor de toepassing van dit besluit wordt verstaan onder:

- 1° KB vervoer: het koninklijk besluit van 22 oktober 2017 betreffende het vervoer van gevaarlijke goederen van klasse 7;
- 2° KB categorisering: het koninklijk besluit van 17 oktober 2011 betreffende de categorisering en de definiëring van veiligheidszones in de nucleaire installaties en de nucleaire vervoerbedrijven;
- 3° KB RAMAS: het koninklijk besluit van 17 maart 2024 betreffende de beveiliging van radioactieve stoffen en bepaalde kernmaterialen;
- 4° KB berging: het koninklijk besluit van 17 maart 2024 betreffende de beveiliging van inrichtingen voor de bovengrondse berging van radioactief afval;
- 5° KB fysieke beveiliging: het koninklijk besluit van 17 oktober 2011 betreffende de fysieke beveiliging van het kernmateriaal en de nucleaire installaties;
- 6° CCB: het Centrum voor Cybersecurity België opgericht bij koninklijk besluit van 10 oktober 2014;
- 7° NCB: de nucleaire cyberbeveiliging zoals gedefinieerd in artikel 1 van de wet van 15 april 1994;
- 8° Inrichting:
 - a. een nucleaire installatie zoals gedefinieerd door artikel 1bis van de wet van 15 april 1994 of
 - b. een inrichting zoals gedefinieerd door het Algemeen Reglement of
 - c. een nucleair vervoerbedrijf zoals bedoeld in het KB categorisering, met uitzondering van de voertuigen;
- 9° Exploitant:
 - a. Een exploitant in de zin van het algemeen reglement of
 - b. Een exploitant van een nucleaire installatie of van een nucleair vervoerbedrijf in de zin van het KB categorisering;
- 10° Kwetsbaarheid: kwetsbaarheid in de zin van artikel 8, 15° van de wet van 26 april 2024 tot vaststelling van een kader voor de beveiliging van netwerk- en

§2. Pour l'application du présent arrêté, on entend par :

- 1° AR transport : l'arrêté royal du 22 octobre 2017 concernant le transport de marchandises dangereuses de la classe 7 ;
- 2° AR catégorisation : l'arrêté royal du 17 octobre 2011 relatif à la catégorisation et à la définition de zones de sécurité au sein des installations nucléaires et des entreprises de transport nucléaire ;
- 3° AR RAMAS : l'arrêté royal du 17 mars 2024 portant sur la sécurité des substances radioactives et de certaines matières nucléaires ;
- 4° AR stockage : l'arrêté royal du 17 mars 2024 portant sur la sécurité des établissements pour le stockage en surface des déchets radioactifs ;
- 5° AR protection physique : l'arrêté royal du 17 octobre 2011 relatif à la protection physique des matières nucléaires et des installations nucléaires ;
- 6° CCB : le Centre pour la Cybersécurité Belgique, créé par l'arrêté royal du 10 octobre 2014 ;
- 7° CSN : la cybersécurité nucléaire telle que définie à l'article 1er de la loi du 15 avril 1994 ;
- 8° Etablissement :
 - a. une installation nucléaire telle que définie par l'article 1bis de la loi du 15 avril 1994 ou
 - b. un établissement tel que défini par le Règlement général ou
 - c. une entreprise de transport nucléaire au sens de l'AR catégorisation, à l'exception des véhicules ;
- 9° Exploitant :
 - a. un exploitant au sens du règlement général ou
 - b. un exploitant d'une installation nucléaire ou d'une entreprise de transport de matières nucléaires au sens de l'AR catégorisation ;
- 10° Vulnérabilité : la vulnérabilité au sens de l'article 8, 15°, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information

informatiesystemen van algemeen belang voor de openbare veiligheid;

11° Conformiteitsbeoordelingsinstantie: een conformiteitsbeoordelingsinstantie in de zin van artikel 8, 53° , van de NIS2-wet;

12° Nationale accreditatie-instantie: een nationale accreditatie-instantie in de zin van artikel 8, 51° van de NIS2-wet ;

13° KB tot uitvoering van de NIS2-wet: Koninklijk besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

d'intérêt général pour la sécurité publique ;

11° Organisme d'évaluation de la conformité : un organisme d'évaluation de la conformité au sens de l'article 8, 53°, de la loi NIS2 ;

12° Organisme national d'accréditation : un organisme national d'accréditation au sens de l'article 8, 51° de la loi NIS2 ;

13° AR d'exécution de la loi NIS2 : Arrêté royal du 9 juin 2024 exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Artikel 2. Toepassingsgebied

§1. Dit besluit is van toepassing op de netwerk- en informatiesystemen - van inrichtingen voor zover deze netwerk- en informatiesystemen, voor deze inrichtingen, het beheer, de controle of de veiligstelling van kernmateriaal of van radioactieve stoffen in deze inrichtingen rechtstreeks of onrechtstreeks mogelijk maken, waarborgen of ondersteunen.

§2. Onderhavig besluit is niet van toepassing op netwerk- en informatiesystemen van inrichtingen van de Belgische krijgsmacht.

§3. De netwerk- en informatiesystemen bedoeld in §1 die beantwoorden aan de bepalingen van de NIS2-wet moeten niet voldoen aan de bepalingen van dit besluit. Echter deze netwerken en informatiesystemen die volledig geïntegreerd zijn in het netwerk- en informatiesysteem van een andere inrichting die uitsluitend onder dit besluit valt, dienen te voldoen aan de bepalingen van dit besluit.

§4. Het Agentschap en het CCB wisselen informatie uit met betrekking tot de inrichtingen die als essentiële of belangrijke entiteit beschouwd worden volgens de bepalingen van de NIS2-wet.

Hoofdstuk II: De categorieën van de netwerk- en informatiesystemen

Article 2. Champ d'application

§1^{er}. Le présent arrêté s'applique aux réseaux et systèmes d'information - des établissements pour autant que, pour ces établissements, ces réseaux et systèmes d'information permettent, assurent ou appuient, directement ou indirectement, la gestion, le contrôle ou la sécurisation des matières nucléaires ou des substances radioactives qui s'y trouvent.

§2. Le présent arrêté ne s'applique pas aux réseaux et systèmes d'information des établissements des forces armées belges.

§3. Les réseaux et systèmes d'information visés au §1 qui répondent aux exigences de la loi NIS2 ne doivent pas satisfaire aux dispositions du présent arrêté. Toutefois, ceux de ces réseaux et systèmes d'information qui sont entièrement intégrés dans le réseau et le système d'information d'un autre établissement relevant exclusivement du présent arrêté doivent se conformer aux dispositions du présent arrêté.

§4. L'Agence et le CCB échangent des informations sur les établissements considérés comme des entités essentielles ou importantes en vertu des dispositions de la loi NIS2.

Chapitre II : Les catégories de réseaux et de systèmes d'information

Artikel 3. Indeling in categorieën

§1. De netwerk- en informatiesystemen worden onderverdeeld in vijf categorieën op basis van de mate van hun kritichtheid, d.w.z. het vermogen waarover zij of de bijbehorende diensten moeten beschikken om bestand te zijn tegen acties die de beschikbaarheid, de authenticiteit, de integriteit of de vertrouwelijkheid van de gegevens die zij opslaan, verzenden of verwerken zouden kunnen compromitteren. Bij de mate van kritichtheid die in aanmerking moet worden genomen, wordt ook rekening gehouden met de mogelijke gevolgen van deze acties op de nucleaire en radiologische veiligheid en beveiliging, alsook met de voldoende garantie die de exploitant moet bieden dat het weerstandsvermogen wordt bereikt en wordt bewaard.

§2. De categorie Cyber-1 wordt toegekend aan:

- a) de netwerk- en informatiesystemen die instaan voor de supervisie en aansturing van processen die rechtstreeks of onrechtstreeks het beheer, de controle of de veiligstelling van het kernmateriaal, met inbegrip van de nucleaire documenten mogelijk maken, waarborgen of ondersteunen en die zich bevinden in de zeer hoog beschermde zone, de hoog beschermde zone, beschermde zone of vitale zone zoals gedefinieerd in artikel 2 van het KB categorisering;
- b) de netwerk- en informatiesystemen van een nucleair vervoerbedrijf die de informatie met betrekking tot de diverse fasen van de organisatie en de voorbereiding van de transporten van kernmaterialen behorende tot de vervoersgroep A, zoals voorzien in artikel 3 van het KB categorisering, bevatten, behandelen of verzenden;
- c) de netwerk- en informatiesystemen die niet onder a) of b) bedoelde nucleaire documenten gecategoriseerd als "ZEER GEHEIM-NUC" of "GEHEIM-NUC", bevatten, behandelen en verzenden en die zich bevinden in een andere veiligheidszone van de inrichting dan deze bedoeld in punten a) of b);

Article 3. Catégorisation

§1. Les réseaux et systèmes d'information sont répartis en cinq catégories en fonction de leur degré de criticité, c'est-à-dire de la capacité qu'eux-mêmes ou leurs services connexes doivent avoir de résister aux actions qui pourraient compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données qu'ils stockent, transmettent ou traitent. Le degré de criticité à considérer prend également en compte les conséquences possibles de ces actions sur la sûreté et la sécurité nucléaires et radiologiques ainsi que l'assurance plus ou moins grande que l'exploitant doit fournir que la capacité de résistance est atteinte et maintenue.

§2. La catégorie Cyber-1 est attribuée :

- a) aux réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement la gestion, le contrôle ou la sécurisation des matières nucléaires, y compris ce qui concerne les documents nucléaires, et qui se situent en zone très hautement protégée, en zone hautement protégée, en zone protégée ou en zone vitale telles qu'elles sont définies à l'article 2 de l'AR Catégorisation ;
- b) aux réseaux et systèmes d'information d'une d'entreprise de transport nucléaire sur lesquels les informations relatives aux différentes phases d'organisation et de préparation des transports de matières nucléaires appartenant au groupe de transport A, comme prévu à l'article 3 de l'AR catégorisation, sont conservées, traitées ou transmises ;
- c) aux réseaux et systèmes d'information qui contiennent, traitent ou transmettent des documents nucléaires catégorisés TRES SECRET-NUC ou SECRET-NUC non visés aux points a) ou b) et qui se trouvent dans une zone de sécurité de l'établissement autre que celles visées aux points a) ou b);

d) de netwerk- en informatiesystemen die op enigerlei wijze communiceren of verbonden zijn met de veiligheidszones bedoeld in punten a), b) of c).

§3. De categorie Cyber-2 wordt toegekend aan:

- a) de netwerk- en informatiesystemen die instaan voor de supervisie en aansturing van processen die rechtstreeks of onrechtstreeks het beheer, de controle of de veiligstelling van het kernmateriaal, met inbegrip van de nucleaire documenten, mogelijk maken, waarborgen of ondersteunen en die zich bevinden hetzij in de beveiligde zone zoals gedefinieerd in artikel 2 van het KB categorisering, hetzij in de zone bedoeld in artikel 2,§7, van hetzelfde besluit en afgebakend door de interne perimeter, of indien deze afwezig is, de externe perimeter, hetzij buiten een veiligheidszone maar binnen in de nucleaire installatie;
- b) de netwerk- en informatiesystemen van een nucleair vervoerbedrijf die de informatie met betrekking tot de diverse fasen van organisatie en de voorbereiding van de transporten van kernmaterialen behorende tot de vervoersgroep B, zoals voorzien in artikel 3 van het KB categorisering, bevatten, behandelen of verzenden;
- c) de netwerk- en informatiesystemen die niet onder a) of b) bedoelde nucleaire documenten gecategoriseerd als "VERTROUWELIJK-NUC", bevatten, behandelen en verzenden en die zich bevinden in een andere veiligheidszone van de inrichting dan deze bedoeld in punten a) of b);
- d) de netwerk- en informatiesystemen die communiceren met de beveiligde zone, of met de veiligheidszone voorzien in punt c) of met delen van de nucleaire installatie die zich buiten de veiligheidszones bevinden of die er op enigerlei wijze mee verbonden zijn.

§4. De categorie Cyber-3 wordt toegekend aan:

- a) de netwerk- en informatiesystemen die instaan voor de supervisie en aansturing

d) aux réseaux et systèmes d'information qui communiquent avec les zones de sécurité visées aux points a), b) ou c) ou qui y sont reliés d'une quelconque manière.

§3. La catégorie Cyber-2 est attribuée :

- a) aux réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement la gestion, le contrôle ou la sécurisation des matières nucléaires, y compris ce qui concerne les documents nucléaires, et qui se situent soit en zone sécurisée telle qu'elle est définie à l'article 2 de l'AR Catégorisation, soit dans la zone visée à l'article 2 §7 du même arrêté et circonscrite par le périmètre intérieur ou, en l'absence de périmètre intérieur, par le périmètre extérieur, soit en dehors d'une zone de sécurité mais à l'intérieur de l'installation nucléaire ;
- b) aux réseaux et systèmes d'information d'une d'entreprise de transport nucléaire sur lesquels les informations relatives aux différentes phases d'organisation et de préparation des transports de matières nucléaires appartenant au groupe de transport B, comme prévu à l'article 3 de l'AR catégorisation, sont conservées, traitées transmises ;
- c) aux réseaux et systèmes d'information qui contiennent, traitent ou transmettent des documents nucléaires catégorisés CONFIDENTIEL-NUC non visés aux points a) ou b) et qui se trouvent dans une zone de sécurité de l'établissement autre que celles visées aux points a) ou b) ;
- d) aux réseaux et systèmes d'information qui communiquent avec la zone sécurisée, avec la zone de sécurité visée au point c) ou avec les parties de l'installation nucléaire qui se situent à l'extérieur d'une zone de sécurité, ou qui y sont reliés d'une quelconque manière.

§4. La catégorie Cyber-3 est attribuée :

van processen die rechtstreeks of onrechtstreeks het beheer, de controle of de veiligstelling van radioactieve stoffen, met inbegrip van de radiologische beveiligingsdocumenten, mogelijk maken, waarborgen of ondersteunen en die zich bevinden in een beveiligde ruimte van het beveiligingsniveau A volgens het KB RAMAS;

- b) de netwerk- en informatiesystemen die op enigerlei wijze communiceren of verbonden zijn met ruimtes bedoeld onder a).

§5. De categorie Cyber-4 wordt toegekend aan:

- a) de netwerk- en informatiesystemen die instaan voor de supervisie en aansturing van processen die rechtstreeks of onrechtstreeks het beheer, de controle of de veiligstelling van radioactieve stoffen, met inbegrip van de radiologische beveiligingsdocumenten, mogelijk maken, waarborgen of ondersteunen en die zich bevinden in een beveiligde ruimte van het niveau B of C volgens het KB RAMAS;
- b) de netwerk- en informatiesystemen die instaan voor de supervisie en aansturing van processen die rechtstreeks of onrechtstreeks het beheer, de controle of de veiligstelling van radioactieve stoffen, met inbegrip van de radiologische beveiligingsdocumenten, mogelijk maken, waarborgen of ondersteunen en die zich bevinden in een inrichting voor de bovengrondse berging van radioactief afval en waarvan de beveiliging geregeld is in het KB berging.
- c) de netwerk- en informatiesystemen die op enigerlei wijze communiceren of verbonden zijn met de ruimtes en plaatsen bedoeld onder a) en b).

§6. De categorie Cyber-5 wordt toegekend aan:

- a) de netwerk- en informatiesystemen die instaan voor de supervisie en aansturing van processen die rechtstreeks of onrechtstreeks het beheer, de controle of de veiligstelling van radioactieve stoffen die behoren tot de categorieën 4 of 5 volgens het KB RAMAS mogelijk maken,

a) aux réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement la gestion, le contrôle ou la sécurisation des substances radioactives, y compris ce qui concerne les documents de sécurité radiologique, et qui se situent dans un espace sécurisé du niveau de sécurité A au sens de l'AR RAMAS ;

b) aux réseaux et systèmes d'information qui communiquent avec les espaces mentionnés au point a) ou qui y sont reliés d'une quelconque manière.

§5. La catégorie Cyber-4 est attribuée :

a) aux réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement la gestion, le contrôle ou la sécurisation des substances radioactives, y compris ce qui concerne les documents de sécurité radiologique, et qui se situent dans un espace sécurisé du niveau de sécurité B ou C au sens de l'AR RAMAS ;

b) aux réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement la gestion, le contrôle ou la sécurisation des substances radioactives, y compris ce qui concerne les documents de sécurité radiologique, et qui se situent dans un établissement pour le stockage en surface des déchets radioactifs dont la sécurité est réglée par l'AR stockage.

c) aux réseaux et systèmes d'information qui communiquent avec les espaces et lieux mentionnés aux points a) et b) ou qui y sont reliés d'une quelconque manière.

§6. La catégorie Cyber-5 est attribuée :

a) aux réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement la gestion, le contrôle ou la sécurisation des

- waarborgen of ondersteunen en die zich bevinden in de inrichting;
- b) de netwerk- en informatiesystemen die instaan voor de supervisie en aansturing van processen die rechtstreeks of onrechtstreeks het beheer, de controle of de veiligstelling van radioactieve stoffen mogelijk maken, waarborgen of ondersteunen en die zich bevinden in de inrichtingen en die niet onder de categorieën Cyber 1 tot 4 vallen.
- c) de netwerk- en informatiesystemen die op enigerlei wijze communiceren of verbonden zijn met de plaatsen bedoeld ander a) en b).

substances radioactives qui appartiennent aux catégories 4 ou 5 au sens de l'AR RAMAS, et qui se situent dans l'établissement ;

- b) aux réseaux et systèmes d'information qui assurent la supervision et le pilotage des processus qui permettent, assurent ou appuient directement ou indirectement la gestion, le contrôle ou la sécurisation des substances radioactives, qui se situent dans les établissements, et qui ne tombent pas sous une des autres catégories ;
- c) aux réseaux et systèmes d'information qui communiquent ou qui sont reliés d'une quelconque manière avec les lieux mentionnés aux points a) et b).

Artikel 4. Beveiligingsniveaus

§1. Aan elke categorie wordt een nucleaire cyberbeveiligingsniveau (hierna "beveiligingsniveau") A, B, C en D toegekend, waarbij A het hoogste beveiligingsniveau vertegenwoordigt.

§2. Aan de netwerk- en informatiesystemen van de categorie cyber-1 wordt hierna beveiligingsniveau A toegekend. Voor dit beveiligingsniveau gelden de essentiële NCB-maatregelen.

§3. Aan de netwerk- en informatiesystemen van de categorieën Cyber-2 en Cyber-3 wordt het beveiligingsniveau B toegekend. Voor dit beveiligingsniveau gelden de belangrijke NCB-maatregelen.

§4. Aan de netwerk- en informatiesystemen van de categorie Cyber-4 wordt het beveiligingsniveau C toegekend. Voor dit beveiligingsniveau gelden de basis NCB-maatregelen.

§5. Aan de netwerk- en informatiesystemen van de categorie Cyber-5 wordt het beveiligingsniveau D toegekend. Voor dit beveiligingsniveau gelden de NCB-maatregelen van behoedzaam beheer waarvan de principes bepaald worden conform artikel 17sexies, §2, van de wet van 15 april 1994.

Article 4. Niveaux de sécurité

§1^{er}. Chaque catégorie se voit attribuer un niveau de cybersécurité nucléaire (ci-après dénommé « niveau de sécurité ») A, B, C et D, A représentant le niveau de sécurité le plus élevé.

§2. Le niveau de sécurité A est attribué aux réseaux et systèmes d'information de la catégorie Cyber-1. Les mesures de CSN essentielles s'appliquent à ce niveau de sécurité.

§3. Le niveau de sécurité B est attribué aux réseaux et systèmes d'information des catégories Cyber-2 et Cyber-3. Les mesures de CSN importantes s'appliquent à ce niveau de sécurité.

§4. Le niveau de sécurité C est attribué aux réseaux et systèmes d'information de la catégorie Cyber-4. Les mesures de CSN de base s'appliquent à ce niveau de sécurité.

§5. Le niveau de sécurité D est attribué aux réseaux et systèmes d'information de la catégorie Cyber-5. S'appliquent à ce niveau de sécurité les mesures de CSN de gestion prudente, dont les principes sont déterminés conformément à l'article 17sexies, §2, de la loi du 15 avril 1994.

§6. Indien in de inrichting netwerk- en informatiesystemen van verschillende categorieën aanwezig zijn, wordt het beveiligingsniveau van de hoogste categorie toegekend tenzij de exploitant kan aantonen dat de netwerk- en informatiesystemen voldoende onafhankelijk zijn van elkaar.

Artikel 5. Bepalingen van toepassing op categorie Cyber-5

Enkel de artikelen 1 tot en met 4 zijn van toepassing op de netwerk- en informatiesystemen die volgens artikel 3 behoren tot de categorie Cyber-5.

Hoofdstuk III: Nucleaire cyberbeveiliging: principes, verantwoordelijkheden en algemene bepalingen.

Artikel 6. Algemene verplichtingen van de exploitant

§1. De exploitant van de inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorieën Cyber-1 tot en met Cyber-4 voert een nucleair cyberbeveiligingssysteem (hierna "NCB-systeem") in dat eigen is aan zijn inrichting en onderhoudt dit systeem.

De exploitant ontwerpt het NCB-systeem zodanig dat het vereiste beveiligingsniveau van de betrokken netwerk- en informatiesystemen wordt bereikt. Dit bereikte niveau moet beter gewaarborgd worden naarmate het beschouwde beveiligingsniveau hoger is.

Het NCB-systeem is, in verhouding tot het beveiligingsniveau gebaseerd en gebouwd op de naleving van de relevante bepalingen van dit besluit, op de evaluatie van de cyber risico's waaraan de netwerk- en informatiesystemen van de inrichting zouden kunnen worden blootgesteld, en op de naleving van het geheel van goede praktijken, technologieën en referentiedocumenten met betrekking tot cyberbeveiliging, in het bijzonder de nucleaire cyberbeveiliging.

Het NCB-systeem voorziet in de organisatorische, technische en operationele NCB-maatregelen die noodzakelijk, passend en evenredig zijn met het vastgestelde

§6. Si l'établissement comporte des réseaux et systèmes d'information de différentes catégories, le niveau de sécurité correspondant à la catégorie la plus élevée leur est attribué, sauf si l'exploitant peut démontrer que les réseaux et systèmes d'information sont suffisamment indépendants.

Article 5. Dispositions applicables à la catégorie Cyber-5

Seuls les articles 1 à 4 s'appliquent aux réseaux et système d'information qui, aux termes de l'article 3, relèvent de la catégorie Cyber-5.

Chapitre III : Cybersécurité nucléaire : principes, responsabilités et dispositions générales.

Article 6. Obligations générales de l'exploitant

§1^{er}. L'exploitant de l'établissement dont les réseaux et systèmes d'information sont classés dans les catégories Cyber-1 à Cyber-4, établit et maintient un système de cybersécurité nucléaire (ci-après « système de CSN ») propre à son établissement.

L'exploitant conçoit le système de CSN de manière telle que le niveau de sécurité requis des réseaux et système d'information concernés soit atteint, et que cette atteinte soit d'autant mieux garantie que le niveau de CSN considéré est élevé.

Le système de CSN est basé et construit, à proportion du niveau de sécurité, sur l'observation des dispositions pertinentes du présent arrêté, sur l'évaluation des cyber-risques dont les réseaux et systèmes d'information de l'établissement pourraient être l'objet, ainsi que sur l'observation de l'ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la cybersécurité, et spécialement à la cybersécurité nucléaire.

Le système de CSN prévoit les mesures organisationnelles, techniques et opérationnelles de CSN qui sont nécessaires, appropriées et proportionnées au niveau de

beveiligingsniveau en, voor zover aangegeven in §2, met de evaluatie van de cyberrisico's. Deze NCB-maatregelen streven ernaar om het vastgestelde beveiligingsniveau te bereiken en te handhaven, om de cyberrisico's waaraan de netwerk- en informatiesystemen van de inrichting worden blootgesteld te beheren, rekening houdend met de huidige beschikbare kennis, alsook om de cyberincidenten die hen zouden kunnen treffen te voorkomen of de gevolgen ervan te beperken.

§2. De evaluatie van de cyberrisico's, vermeld in §1, heeft betrekking op de cyberrisico's die worden bepaald door de dreigingen en kwetsbaarheden waaraan de netwerk- en informatiesystemen van de inrichting zouden kunnen worden blootgesteld. Ze gaat gepaard met de volgende acties en maatregelen:

- 1° de verplichting voor de afgevaardigde voor NCB om overleg te plegen met de natuurlijke persoon die belast is met het toezicht op de naleving van de regels inzake fysieke beveiliging en nucleaire of radiologische beveiliging in de inrichting met betrekking tot de raakvlakken tussen de risico's waarop enerzijds het NCB-systeem en anderzijds de beveiligingsregels van de inrichting een antwoord moeten bieden;
- 2° de verplichting van de exploitant die kennis heeft van een indirecte of specifieke dreiging tegen de netwerk- en informatiesystemen van zijn inrichting, om de adequaatheid van het NCB-systeem te evalueren en, indien nodig, de NCB-maatregelen aan te passen aan de specificiteit en de aard van deze dreiging of de nodige aanvullende NCB-maatregelen te nemen.

§3. De exploitant documenteert het NCB-systeem in een NCB-dossier. Om dit dossier samen te stellen vraagt hij eerst het advies van de afgevaardigde voor nucleaire cyberbeveiliging.

§4. Het NCB-systeem wordt door het Agentschap erkend.

Artikel 7. Beheerssysteem

sécurité déterminé ainsi que, dans la mesure indiquée au §2, à l'évaluation des cyber-risques. Ces mesures de CSN tendent à atteindre et à maintenir le niveau de sécurité, à gérer les cyber-risques auxquels sont exposés les réseaux et système d'information de l'établissement, compte tenu de l'état des connaissances, ainsi qu'à prévenir les cyber-incidents pouvant les affecter ou en limiter l'impact.

§2. L'évaluation des cyber-risques mentionnée au §1^{er} porte sur les cyber-risques qui sont déterminés par les menaces et les vulnérabilités pouvant affecter les réseaux et systèmes d'information de l'établissement. Elle s'accompagne des actions et mesures suivantes :

- 1° l'obligation du délégué à la CSN de se concerter avec la personne physique chargée de veiller à l'observation des règles de protection physique et de sécurité nucléaire ou radiologique dans l'établissement quant aux interfaces entre les risques auxquels entendent répondre d'une part le système de CSN et d'autre part les règles de sécurité de l'établissement ;
- 2° l'obligation pour l'exploitant qui a connaissance d'une menace circonstancielle ou particulière contre les réseaux et système d'information de son établissement d'évaluer l'adéquation du système de CSN et, si nécessaire, d'adapter les mesures de CSN aux spécificités et à la nature de cette menace ou de prendre les mesures de CSN complémentaires qui s'imposent.

§3. L'exploitant documente le système de CSN dans un dossier de CSN. Pour l'établir, il demande d'abord l'avis du délégué à la cybersécurité nucléaire.

§4. Le système de CSN est agréé par l'Agence.

Article 7. Système de gestion

De exploitant integreert het NCB-systeem op structurele wijze in de inrichting.

L'exploitant intègre le système de CSN de manière structurée au sein de l'établissement.

Artikel 8. De afgevaardigde voor nucleaire cyberbeveiliging

Article 8. Le délégué à la cybersécurité nucléaire

§1. De exploitant stelt binnen zijn inrichting of organisatie ten minste één afgevaardigde voor nucleaire cyberbeveiliging (hierna de "afgevaardigde voor NCB") aan die, al dan niet als personeelslid, voor de exploitant, de inrichting of de organisatie werkt op een duurzame wijze.

§1^{er}. L'exploitant désigne au sein de son établissement ou organisation au moins un délégué à la cybersécurité nucléaire (ci-après "le délégué à la CSN") qui travaille, comme membre du personnel ou non, pour l'exploitant, l'établissement ou l'organisation de manière durable.

§2. De afgevaardigde voor NCB wordt aangesteld op grond van zijn professionele kwaliteiten en zijn deskundigheid. De afgevaardigde moet de kwaliteiten en deskundigheid kunnen aantonen aan de hand van certificaten, getuigschriften, opleidingen, diploma's, ervaring of vorming.

§2. Le délégué à la CSN est désigné sur la base de ses qualifications professionnelles et de son expertise. Il doit pouvoir justifier ces qualifications et cette expertise par des certificats, des attestations, des formations, des diplômes, son expérience ou sa formation.

§3. Het Agentschap keurt de aanstelling van de afgevaardigde voor NCB goed. Daartoe dient de exploitant de identificatiegegevens van de afgevaardigde voor NCB alsook de informatie waaruit de kwaliteiten en ervaring blijken op grond waarvan de afgevaardigde werd aangeduid mee te delen aan het Agentschap. Het Agentschap kan voorwaarden opleggen aan deze goedkeuring.

§3. L'Agence approuve la désignation du délégué à la CSN. À cet effet, l'exploitant lui communique les données d'identification du délégué à la CSN, ainsi que les données attestant des qualifications et de l'expérience en raison desquelles il est désigné. L'Agence peut soumettre l'approbation à des conditions.

§4. Wijzigingen met betrekking tot de aanstelling van de afgevaardigde voor NCB worden aan het Agentschap gemeld.

§4. Les modifications concernant la désignation du délégué à la CSN sont notifiées à l'Agence.

§5. Het Agentschap kan aanbevelingen of een technisch reglement opstellen betreffende de praktische modaliteiten voor aanstelling en de goedkeuring alsook voor het melden van wijzigingen..

§5. L'Agence peut adopter des recommandations ou un règlement technique concernant les modalités pratiques de la désignation et de l'approbation ainsi que pour la notification des modifications.

Artikel 9. Opdrachten van de afgevaardigde voor nucleaire cyberbeveiliging.

Article 9. Missions du délégué à la cyber sécurité nucléaire.

§1. De afgevaardigde voor NCB zorgt voor het opzetten en onderhouden van het NCB-systeem, voor rekening en onder verantwoordelijkheid van de exploitant. De exploitant zorgt ervoor dat de afgevaardigde voor NCB naar behoren en tijdig betrokken

§1^{er}. Le délégué à la CSN veille à l'établissement et au maintien du système de CSN, pour le compte de l'exploitant et sous la responsabilité de celui-ci. L'exploitant fait en sorte que le délégué à la CSN soit impliqué de manière appropriée et en temps utile dans les

wordt bij alle aangelegenheden die verband houden met de nucleaire cyberbeveiliging.

questions relatives à la cybersécurité nucléaire.

§2. De exploitant ondersteunt de afgevaardigde voor NCB bij het uitvoeren van zijn taken en voorziet hem van de nodige tijd en middelen om zijn taken uit te voeren en zijn deskundigheid op peil te houden.

§2. L'exploitant soutient le délégué à la CSN dans l'exercice de ses tâches et met à sa disposition le temps et les ressources nécessaires à leur exécution et au maintien de son expertise.

§3. De afgevaardigde voor NCB brengt rechtstreeks verslag uit aan de exploitant of zijn afgevaardigde.

§3. Le délégué à la CSN rapporte directement à l'exploitant ou à son délégué.

§4. De afgevaardigde voor NCB informeert en adviseert de exploitant en zijn medewerkers over alle aangelegenheden en hun verplichtingen inzake NCB.

§4. Le délégué à la CSN informe et conseille l'exploitant et ses collaborateurs sur toutes les questions relatives à la CSN et sur leurs obligations en la matière.

§5. De exploitant consulte de afgevaardigde voor NCB wanneer beslissingen worden genomen die mogelijk een belangrijke impact kunnen hebben op de NCB binnen de inrichting. De afgevaardigde voor NCB moet onmiddellijk geconsulteerd worden wanneer er zich een cyberincident voordoet.

§5. L'exploitant consulte le délégué à la CSN lors de la prise de décisions susceptibles d'avoir une incidence importante sur la CSN au sein de l'établissement. Le délégué à la CSN doit être consulté immédiatement en cas de cyber-incident.

§6. De afgevaardigde voor NCB ziet toe op de uitvoering en de naleving van de NCB-maatregelen.

§6. Le délégué à la CSN veille à la mise en œuvre et à l'observation des mesures de CSN.

§7. Onverminderd de eindverantwoordelijkheid van de exploitant kan de afgevaardigde voor NCB aangesteld worden als interne en externe contactpersoon voor alle zaken betreffende NCB.

§7. Sans préjudice de la responsabilité finale de l'exploitant, le délégué à la CSN peut être désigné comme personne de contact interne et externe pour toutes les questions de CSN.

§8. De afgevaardigde voor NCB besteedt de nodige aandacht aan bewustmaking en opleiding van de medewerkers van de exploitant.

§8. Le délégué à la CSN accorde l'attention nécessaire à la conscientisation et à la formation des collaborateurs de l'exploitant.

§9. De afgevaardigde voor NCB zorgt ervoor dat periodiek de nodige audits worden uitgevoerd in overeenstemming met artikel 23.

§9. Le délégué à la CSN s'assure de la réalisation des audits périodiques nécessaires conformément à l'article 23.

§10. Indien de afgevaardigde voor NCB vaststelt dat het NCB-systeem niet correct wordt toegepast, stelt hij de exploitant hiervan onverwijld in kennis en stelt NCB-maatregelen voor om een correcte toepassing ervan te verzekeren. Hij zorgt ervoor dat de door de

§10. Si le délégué à la CSN constate que le système de CSN n'est pas appliqué correctement, il en informe l'exploitant sans délai, et propose les mesures de CSN visant à en garantir la bonne application. Il vérifie la mise en œuvre des mesures de CSN imposées par l'exploitant.

exploitant opgelegde NCB-maatregelen uitgevoerd worden.

§11. De afgevaardigde voor NCB stelt ten behoeve van de exploitant jaarlijks een verslag op en houdt het ter beschikking van het Agentschap.

Dit jaarverslag omvat minstens:

1. een algemeen overzicht van de toestand inzake NCB en de genomen NCB-maatregelen en een overzicht van de evolutie in het afgelopen jaar en de nog te realiseren doelstellingen;
2. een samenvatting van de adviezen die door de afgevaardigde voor NCB overgemaakt werden aan de exploitant en het gevolg dat eraan werd gegeven;
3. een overzicht van de werkzaamheden verricht door de afgevaardigde voor NCB;
4. een overzicht van de genomen bewustwordingsinitiatieven en gevoerde campagnes ter bevordering van de NCB;
5. een overzicht van gevolgde en de voorziene nog te volgen opleidingen;
6. een overzicht van de uitgevoerde interne en externe audits van de NCB en de opvolging van de daaruit volgende acties.

§12. Het Agentschap kan de minimale inhoud van dit jaarverslag verder bepalen in een technisch reglement.

§13. De afgevaardigde voor NCB kan zich laten bijstaan door derden of kan hun advies inwinnen.

§14. Onverminderd artikel 6, §2, 1° overlegt de afgevaardigde voor NCB met de :

1° natuurlijke persoon die belast is met het toezicht op de naleving van de regels inzake fysieke beveiliging en nucleaire of radiologische beveiliging in de inrichting, om rekening te houden met en het beheer van de interfaces tussen het NCB-systeem en, naargelang het geval, het fysieke beveiligingssysteem of het radiologische beveiligingssysteem;

2° met het hoofd van de dienst voor fysieke controle van de inrichting om rekening te houden met het beheer van de interfaces tussen het NCB-systeem en nucleaire of

§11. Le délégué à la CSN établit un rapport annuel destiné à l'exploitant et le tient à la disposition de l'Agence.

Ce rapport annuel contient au moins :

1. un aperçu général de la situation en matière de CSN et des mesures de CSN adoptées et un aperçu de l'évolution au cours de l'année écoulée et des objectifs qu'il reste à réaliser ;
2. un résumé des avis transmis par le délégué à la CSN à l'exploitant et des suites qui leur ont été données ;
3. un aperçu des activités réalisées par le délégué à la CSN ;
4. un relevé des initiatives prises à des fins de conscientisation et des campagnes menées pour promouvoir la CSN ;
5. un relevé des formations suivies et de celles qu'il est prévu de suivre ;
6. un relevé des audits de CSN internes et externes réalisés et un aperçu des actions qui en découlent.

§12. L'Agence peut spécifier le contenu minimal de ce rapport annuel dans un règlement technique.

§13. Le délégué à la CSN peut se faire assister par des tiers ou leur demander conseil.

§14. Sans préjudice de l'article 6, §2, 1°, le délégué à la CSN se consulte avec :

1° la personne physique chargée de veiller à l'observation des règles de protection physique et de sécurité nucléaire ou radiologique dans l'établissement pour la prise en compte et la gestion des interfaces entre le système de CSN et, selon le cas, le système de protection physique ou le système de sécurité radiologique ;

2° le chef du service contrôle physique de l'établissement pour la prise en compte et la gestion des interfaces entre le système de CSN et la sûreté nucléaire ou radiologique et la radioprotection.

radiologische veiligheid en
stralingsbescherming.

§15. De opdrachten die bij toepassing van dit artikel aan de afgevaardigde voor NCB worden toegewezen doen in geen enkel opzicht afbreuk aan de autoriteit en de verantwoordelijkheden van de exploitant. Deze verantwoordelijkheden kunnen niet worden gedelegeerd.

§16. Het Agentschap kan aanbevelingen of een technisch reglement opstellen waarin de taken en verantwoordelijkheden van de afgevaardigde voor NCB worden gespecificeerd.

Artikel 10. Permanente vorming

§1. De exploitant ziet erop toe dat een permanente vorming betreffende NCB wordt gewaarborgd en kan gevolgd worden door zijn personeel, in het bijzonder door de afgevaardigde voor NCB.

§2. De exploitant informeert en geeft opleiding aan alle gebruikers van zijn netwerk- en informatiesystemen, met inbegrip van zijn eigen werknemers en externe medewerkers, over zijn nucleair cyberbeveiligingsbeleid en de daaruit voortvloeiende NCB-maatregelen. In het bijzonder voorziet hij sensibiliseringscampagnes en vorming zodat bedreigingen binnen de inrichting kunnen worden herkend en gemeld.

Hoofdstuk IV: Nucleaire cyberbeveiligingsmaatregelen

Artikel 11. Algemeenheden

De nucleaire cyberbeveiligingsmaatregelen gelden onverminderd de toepasselijke regelgeving met betrekking tot de nucleaire en radiologische beveiligingsdocumenten.

Artikel 12. Essentiële nucleaire cyberbeveiligingsmaatregelen

§1. De volgende cyberbeveiligingsmaatregelen vormen de essentiële NCB-maatregelen:

§15. Les missions attribuées au délégué à la CSN en application de cet article ne préjudicient en rien à l'autorité et aux responsabilités de l'exploitant. Ces responsabilités ne peuvent pas être déléguées.

§16. L'Agence peut adopter des recommandations ou un règlement technique précisant les tâches et les responsabilités du délégué à la CSN.

Article 10. Formation continue

§1^{er}. L'exploitant veille à ce qu'une formation continue à la CSN soit assurée et puisse être suivie par son personnel, en particulier par le délégué à la CSN.

§2. L'exploitant informe et forme tous les utilisateurs de ses réseaux et systèmes d'information, y compris ses propres employés et le personnel extérieur, à propos de la politique de cybersécurité nucléaire de l'établissement et des mesures de CSN qui en découlent. En particulier, il organise des campagnes de sensibilisation et des formations afin que les menaces puissent être reconnues et signalées au sein de l'établissement.

Chapitre IV : Mesures de cybersécurité nucléaire

Article 11. Généralités

Les mesures de cybersécurité nucléaire sont applicables sans préjudice de la réglementation applicable aux documents de sécurité nucléaire et radiologique.

Article 12. Mesures de cybersécurité nucléaire essentielles

§1^{er}. Les mesures de cybersécurité suivantes constituent des mesures de CSN essentielles :

A) Identificatiemaatregelen

- 1° de exploitant maakt de inventarisatie op van fysieke apparaten en systemen, van gebruikte softwareplatformen en toepassingen en bepaalt hun prioriteit. Deze inventaris wordt bijgehouden, geëvalueerd en continu bijgewerkt;
- 2° de exploitant identificeert leveranciers van producten en diensten en de hieraan verbonden risico's voor de netwerk- en informatiesystemen;
- 3° de exploitant brengt de communicatie- en gegevensstromen in kaart en beveiligt deze alsook de verbindingen met externe netwerk- en informatiesystemen;
- 4° de exploitant stelt de rollen, verantwoordelijkheden en bevoegdheden vast voor het gehele personeel alsook belanghebbende derden.

B) Beschermingsmaatregelen

- 1° de exploitant beheert en beschermt de fysieke toegang tot zijn netwerk- en informatiesystemen en neemt maatregelen ter garantie van die toegang in noodsituaties. Hij beheert de toegangsrechten en machtigingen voor alle gebruikers tot zijn netwerk- en informatiesystemen. Hij neemt bijkomende beveiligingsmaatregelen voor gebruikers met verhoogde toegangsrechten;
- 2° de exploitant beheert alle toegangen op afstand tot zijn netwerk- en informatiesystemen door middel van multifactorauthenticatie, beveiligt de draadloze toegangspunten tot die systemen en stelt de nodige gebruiksbeperkingen, verbinderingsvereisten, implementatierichtlijnen en autorisaties voor toegang op afstand tot die systemen vast, documenteert en implementeert deze;
- 3° Ter bescherming van zijn netwerk- en informatiesystemen neemt de exploitant minstens de volgende maatregelen:
 - a. de exploitant beschermt de integriteit van zijn netwerk- en informatiesystemen door netwerksegmentatie en -scheiding;

A) Mesures d'identification

- 1° L'exploitant dresse un inventaire des dispositifs physiques et des systèmes, des plateformes logicielles et des applications utilisées et détermine leur priorité. Cet inventaire est maintenu, révisé et mis à jour en permanence ;
- 2° L'exploitant identifie les fournisseurs de produits et de services et les risques associés pour les réseaux et systèmes d'information ;
- 3° L'exploitant schématise et sécurise les flux de communication et de données ainsi que les connexions aux réseaux et systèmes d'information externes ;
- 4° L'exploitant détermine les rôles, les responsabilités et les pouvoirs de l'ensemble du personnel et des tiers intéressés.

B) Mesures de protection

- 1° L'exploitant gère et protège l'accès physique à ses réseaux et systèmes d'information et prend des mesures pour garantir cet accès en cas d'urgence. Il gère les droits d'accès et les autorisations de tous les utilisateurs à ses réseaux et systèmes d'information. Il prend des mesures de sécurité supplémentaires pour les utilisateurs disposant de droits d'accès élevés ;
- 2° L'exploitant gère tous les accès à distance à ses réseaux et à ses systèmes d'information au moyen d'une authentification multifactorielle, sécurise les points d'accès sans fil à ces systèmes et établit, documente et met en œuvre les restrictions d'utilisation, les exigences de connexion, les lignes directrices de mise en œuvre et les autorisations nécessaires pour l'accès à distance à ces systèmes ;
- 3° Pour protéger ses réseaux et systèmes d'information, l'exploitant prend au moins des mesures suivantes :
 - a. L'exploitant protège l'intégrité de ses réseaux et systèmes d'information par la segmentation et la séparation de ceux-ci ;

- b. de exploitant voert de controles uit om ongeoorloofde wijzigingen van zijn netwerk- en informatiesystemen op te sporen inclusief de integriteit;
- c. de exploitant stelt NCB-eisen aan derden;
- d. de exploitant implementeert NCB in het personeelsbeleid, met inbegrip van de ontwikkeling en handhaving van een procedure voor NCB bij de aanwerving, tijdens het dienstverband en bij de beëindiging van het dienstverband;
- e. de exploitant beschermt de gegevens in het bijzonder de kritieke of gevoelige gegevens over de netwerk- en informatiesystemen;
- f. de exploitant beheert de fysieke middelen en componenten van de netwerk- en informatiesystemen die binnen zijn inrichting werden geïnventariseerd en voorziet de nodige maatregelen om verlies, misbruik, beschadiging of diefstal hiervan tegen te gaan;
- g. de exploitant houdt de ontwikkelings- en testomgeving(en) en de productieomgeving(en) van zijn netwerk- en informatiesystemen gescheiden;
- h. de exploitant ontwikkelt een beheer dat de levenscyclus van de componenten van zijn netwerk- en informatiesystemen omvat;
- i. de exploitant voert back-ups uit van de gegevens en informatie van zijn netwerk- en informatiesystemen, en bewaart, verifieert en test de betrouwbaarheid en de integriteit ervan;
- j. de exploitant houdt de door het netwerk- en informatiesysteem van de inrichting gegenereerde gegevens en informatie bij en evalueert deze.

C) Detectiemaatregelen

- 1° de exploitant neemt de maatregelen die toelaten om cyberincidenten en potentiële cyberincidenten te kunnen vaststellen, evalueren en analyseren

- b. L'exploitant effectue des contrôles permettant de détecter les modifications non autorisées de ses réseaux et systèmes d'information, y inclus l'intégrité ;
- c. L'exploitant impose des exigences en matière de CSN envers les tiers ;
- d. L'exploitant met en œuvre la CSN dans la politique de ressources humaines, y compris l'élaboration et la mise à jour d'une procédure de CSN au moment du recrutement, pendant l'emploi et au moment de la cessation d'emploi ;
- e. L'exploitant protège les données en particulier les données critiques ou sensibles sur les réseaux et systèmes d'information ;
- f. L'exploitant gère les ressources physiques et composants des réseaux et systèmes d'information inventoriés dans son établissement et prévoit les mesures nécessaires pour prévenir leur perte, leur utilisation abusive, leur endommagement ou leur vol ;
- g. L'exploitant sépare les environnements de développement et de test des environnements de production de ses réseaux et systèmes d'information ;
- h. L'exploitant met en place une gestion qui couvre le cycle de vie des composants de ses réseaux et systèmes d'information ;
- i. L'exploitant réalise des sauvegardes des données et des informations de ses réseaux et systèmes d'information ; il les préserve, les vérifie et en teste la fiabilité et l'intégrité ;
- j. L'exploitant maintient et évalue les données et les informations générées par les réseaux et systèmes d'information de l'établissement.

C) Mesures de détection

- 1° L'exploitant prend les mesures permettant d'identifier, d'évaluer et d'analyser les cyber-incidents et les cyber incidents potentiels ainsi que d'en déterminer

alsook om de impact ervan op de netwerk- en informatiesystemen van de inrichting te bepalen;

- 2° de exploitant neemt maatregelen om toezicht te houden op de activiteiten binnen de netwerk- en informatiesystemen van de inrichting voor zover dit essentieel is om mogelijke kwetsbaarheden en potentiële cyberincidenten te identificeren of op te sporen, en dit in volledige overeenstemming met de regelgeving met betrekking tot de bescherming van persoonsgegevens. Hij verifieert regelmatig of deze maatregelen passend, noodzakelijk en proportioneel zijn.

D) Respons- en herstelmaatregelen

- 1° de exploitant definieert de nodige processen en criteria om tijdig te reageren op cyberincidenten, om deze te melden in overeenstemming met artikel 16 en om deze te analyseren, te beheersen, de impact ervan te bepalen en de gevolgen ervan te beperken;
- 2° de exploitant stelt een plan op om na een cyberincident de nodige herstellingen aan de netwerk- en informatiesystemen uit te voeren;
- 3° de exploitant documenteert alle cyberincidenten in een incident beheerssysteem. Dit systeem dient steeds ter beschikking van het Agentschap gesteld te worden;
- 4° de exploitant trekt na elk cyberincident lessen uit de reactie op en de herstelmaatregelen genomen naar aanleiding van het cyberincident teneinde zijn NCB-systeem continu te verbeteren.

§2. Het Agentschap kan een technisch reglement opstellen waarin de essentiële NCB-maatregelen verder worden gedetailleerd.

Artikel 13. Belangrijke nucleaire cyberbeveiligingsmaatregelen

§1. De belangrijke NCB-maatregelen zijn de maatregelen genoemd in paragraaf 1 van artikel 12; deze maatregelen kunnen, voor

l'impact sur les réseaux et systèmes d'information de l'établissement ;

- 2° L'exploitant prend les mesures de surveillance des activités au sein des réseaux et systèmes d'information de l'établissement pour autant que cela soit indispensable à l'identification ou à la détection de vulnérabilités et de cyber-incidents potentiels, et ceci dans le plein respect de la réglementation relative à la protection des données personnelles. Il vérifie régulièrement le caractère adéquat, indispensable et proportionné de ces mesures.

D) Mesures de réponse et de rétablissement

- 1° L'exploitant définit les processus et les critères nécessaires pour répondre aux cyber-incidents en temps utile, pour les notifier conformément à l'article 16, pour les analyser, les maîtriser, en déterminer l'impact et en limiter les conséquences ;
- 2° L'exploitant établit un plan de mise en œuvre des rétablissements nécessaires aux réseaux et systèmes d'information à la suite d'un cyber-incident ;
- 3° L'exploitant consigne dans un système de gestion des incidents tous les cyber-incidents. Ce système est tenu à la disposition de l'Agence ;
- 4° Après chaque cyberincident, l'exploitant tire les enseignements de la réponse et des mesures de rétablissement apportées à la suite du cyber-incident, dans un souci d'amélioration continue de son système de CSN.

§2. L'Agence peut adopter un règlement technique détaillant ces mesures de CSN essentielles.

Article 13. Mesures de cybersécurité nucléaire importantes

§1^{er}. Les mesures de CSN importantes sont celles qui sont mentionnées au paragraphe 1 de l'article 12; ces mesures, en tant qu'elles

zover zij van toepassing zijn op beveiligingsniveau B, worden uitgevoerd overeenkomstig artikel 6, § 1, derde lid, en het daarin opgenomen principe dat de genomen maatregelen noodzakelijk, passend en evenredig aan het beveiligingsniveau moeten zijn.

§2. Het Agentschap kan een technisch reglement opstellen waarin deze belangrijke NCB-maatregelen worden gedetailleerd.

Artikel 14. Basis nucleaire cyberbeveiligingsmaatregelen.

§1. De volgende cyberbeveiligingsmaatregelen vormen de basis nucleaire cyberbeveiligingsmaatregelen:

A) Identificatiemaatregelen

- 1° de exploitant maakt de inventarisatie op van fysieke apparaten en systemen, van gebruikte softwareplatformen en toepassingen en bepaalt hun prioriteit. Deze inventaris wordt bijgehouden, geëvalueerd en continu bijgewerkt;
- 2° de exploitant brengt de communicatie- en gegevensstromen in kaart alsook de verbindingen met externe netwerk- en informatiesystemen;

B) Beschermingsmaatregelen

- 1° de exploitant beheert en beschermt de fysieke toegang tot zijn netwerk- en informatiesystemen en neemt maatregelen ter garantie van die toegang in noodsituaties. Hij beheert de toegangsrechten en machtigingen voor alle gebruikers tot zijn netwerk- en informatiesystemen;
- 2° de exploitant beheert alle toegangen op afstand tot zijn netwerk- en informatiesystemen door middel van multifactorauthenticatie, beveiligt de draadloze toegangspunten tot die systemen en stelt de nodige gebruiksbeperkingen, verbinderingsvereisten, implementatierichtlijnen en autorisaties voor toegang op afstand tot die systemen vast, documenteert en implementeert deze;

s'appliquent à un niveau de sécurité B, pourront être déterminées conformément à l'article 6, §1er, alinéa 3, et au principe qu'il énonce selon lequel les mesures prises doivent être nécessaires, appropriées et proportionnées au niveau de sécurité.

§2. L'Agence peut adopter un règlement technique détaillant les mesures de CSN importantes.

Article 14. Mesures de cybersécurité nucléaire de base.

§1. Les mesures de cybersécurité suivantes constituent les mesures de cybersécurité nucléaire de :

A) Mesures d'identification

- 1° L'exploitant dresse un inventaire des dispositifs physiques et des systèmes, des plateformes logicielles et des applications utilisées et détermine leur priorité. Cet inventaire est maintenu, révisé et mis à jour en permanence ;
- 2° L'exploitant schématise et sécurise les flux de communication et de données ainsi que les connexions aux réseaux et systèmes d'information externes ;

B) Mesures de protection

- 1° L'exploitant gère et protège l'accès physique à ses réseaux et systèmes d'information et prend des mesures pour garantir cet accès en cas d'urgence. Il gère les droits d'accès et les autorisations de tous les utilisateurs à ses réseaux et systèmes d'information ;
- 2° L'exploitant prend des mesures de sécurité supplémentaires pour les utilisateurs disposant de droits d'accès élevés. Il gère tous les accès à distance à ses réseaux et à ses systèmes d'information au moyen d'une authentification multifactorielle, sécurise les points d'accès sans fil à ces systèmes et établit, documente et met en œuvre les restrictions d'utilisation, les exigences de connexion, les lignes directrices de mise en œuvre et les

3° Ter bescherming van zijn netwerk- en informatiesystemen neemt de exploitant o.a. volgende maatregelen:

- a. de exploitant beschermt de integriteit van zijn netwerk- en informatiesystemen door netwerksegmentatie en -scheiding;
- b. de exploitant voert de controles uit om ongeoorloofde wijzigingen van zijn netwerk- en informatiesystemen op te sporen;
- c. de exploitant stelt NCB-eisen aan derden;
- d. de exploitant implementeert de NCB in het personeelsbeleid, met inbegrip van de ontwikkeling en handhaving van een procedure voor NCB bij de aanwerving, tijdens het dienstverband en bij de beëindiging van het dienstverband;
- e. de exploitant beschermt de gegevens in het bijzonder de kritieke of gevoelige gegevens op de netwerk- en informatiesystemen;
- f. de exploitant beheert de fysieke middelen en componenten van de netwerk- en informatiesystemen die binnen zijn inrichting werden geïnventariseerd en voorziet de nodige maatregelen om verlies, misbruik, beschadiging of diefstal hiervan tegen te gaan;
- g. de exploitant houdt de ontwikkelings- en testomgeving(en) en de productieomgeving(en) van zijn netwerk- en informatiesystemen gescheiden;
- h. de exploitant houdt de door het netwerk- en informatiesystemen van de inrichting gegenereerde gegevens en informatie bij en evalueert deze.

C) Detectiemaatregelen

De exploitant neemt de maatregelen die toelaten om cyberincidenten en potentiële cyberincidenten te kunnen vaststellen.

autorisations nécessaires pour l'accès à distance à ces systèmes ;

3° Pour protéger ses réseaux et systèmes d'information, l'exploitant prend des mesures notamment celles-ci :

- a. L'exploitant protège l'intégrité de ses réseaux et systèmes d'information par la segmentation et la séparation de ceux-ci ;
- b. L'exploitant effectue des contrôles permettant de détecter les modifications non autorisées de ses réseaux et systèmes d'information ;
- c. L'exploitant impose des exigences en matière de CSN envers les tiers ;
- d. L'exploitant met en œuvre la CSN dans la politique de ressources humaines, y compris l'élaboration et la mise à jour d'une procédure de CSN au moment du recrutement, pendant l'emploi et au moment de la cessation d'emploi ;
- e. L'exploitant protège les données en particulier les données critiques ou sensibles sur les réseaux et systèmes d'information ;
- f. L'exploitant gère les ressources physiques et composants des réseaux et systèmes d'information inventoriés dans son établissement et prévoit les mesures nécessaires pour prévenir leur perte, leur utilisation abusive, leur endommagement ou leur vol ;
- g. L'exploitant sépare les environnements de développement et de test des environnements de production de ses réseaux et systèmes d'information ;
- h. L'exploitant maintient et évalue les données et les informations générées par les réseaux et systèmes d'information de l'établissement.

C) Mesures de détection :

L'exploitant prend les mesures permettant d'identifier les cyber-incidents et les cyber incidents potentiels.

D) Respons- en herstelmaatregelen

- 1° de exploitant definieert de nodige processen en criteria om tijdig te reageren op cyberincidenten, om deze te melden in overeenstemming met artikel 16 en om deze te analyseren, te beheersen, de impact ervan te bepalen en de gevolgen ervan te beperken;
- 2° de exploitant stelt een plan op om na een cyberincident de nodige herstellingen aan de netwerk- en informatiesystemen uit te voeren;
- 3° de exploitant documenteert alle cyberincidenten in een incident beheerssysteem. Dit systeem dient steeds ter beschikking van het Agentschap gesteld worden.

§2. Het Agentschap kan een technisch reglement opstellen waarin deze basis NCB-maatregelen worden gedetailleerd.

Artikel 15. Maatregelen voor het testen van de nucleaire cyberbeveiliging

§1. Om de betrouwbaarheid en de doeltreffendheid te bepalen, test de exploitant de NCB. Hiervoor gaat de exploitant over tot oefeningen. Deze oefeningen bootsen de tactieken, technieken en procedures van reële scenario's na.

§2. Het testen van de NCB moet minimum één maal per drie jaar plaatsvinden voor de inrichtingen waar zich een of meerdere netwerk- en informatiesystemen van het beveiligingsniveau A of B bevinden.

Het testen moet minimum één maal om de vijf jaar plaatsvinden voor de inrichtingen waar zich enkel een of meerdere netwerk- en informatiesystemen van beveiligingsniveau C bevinden.

§3. Wanneer er tekortkomingen worden vastgesteld, neemt de exploitant zo snel mogelijk corrigerende maatregelen.

§4. Na elke test stelt de exploitant binnen de maand een verslag op dat ter beschikking wordt gehouden van het Agentschap.

D) Mesures de réponse et de rétablissement

- 1° L'exploitant définit les processus et les critères nécessaires pour répondre aux cyber-incidents en temps utile, les notifier conformément à l'article 16, les analyser, les maîtriser, en déterminer l'impact et en limiter les conséquences ;
- 2° L'exploitant établit un plan de mise en œuvre des rétablissements des réseaux et systèmes d'information qui sont nécessaires à la suite d'un cyber-incident ;
- 3° L'exploitant consigne dans un système de gestion des incidents tous les cyber-incidents. Ce système est tenu à la disposition de l'Agence.

§2. L'Agence peut adopter un règlement technique détaillant ces mesures de CSN de base.

Article 15. Mesures pour les tests de cybersécurité nucléaire

§1^{er}. L'exploitant teste la CSN pour en déterminer la fiabilité et l'efficacité. À cette fin, l'exploitant procède notamment à des exercices. Ces exercices reproduiront les tactiques, techniques et procédures de scénarios réels.

§2. Ces tests de CSN ont lieu au moins une fois tous les trois ans pour les établissements qui comportent un ou plusieurs réseaux et systèmes d'information de niveau de sécurité A ou B .

Ces tests ont lieu au moins une fois tous les cinq ans pour les établissements qui ne comportent qu'un ou plusieurs réseaux et systèmes d'information de niveau de sécurité C.

§3. En cas de constatation de déficiences, L'exploitant prend des mesures correctives dans les meilleurs délais.

§4. Après chaque test, l'exploitant établit dans le mois un rapport qu'il tient à la disposition de l'Agence.

§5. Het Agentschap kan aanbevelingen of een technisch reglement opstellen betreffende de testmodaliteiten en de minimale inhoud van het verslag.

Artikel 16. Melding van cyber-incidenten

§1. De exploitant meldt cyberincidenten aan het Agentschap en aan het CCB.

§2. Het Agentschap kan aanbevelingen formuleren en een technisch reglement opstellen betreffende de modaliteiten van de melding van de cyberincidenten aan het Agentschap en de informatie die in de melding moet opgenomen worden.

Hoofdstuk V: Uitwisseling van gegevens

Artikel 17. Uitwisseling van gegevens tussen het Agentschap en het CCB in verband met de cyberrisico's en de cyberincidenten waarmee de exploitant wordt of kan worden geconfronteerd

§1. Het Agentschap en het CCB kunnen met elkaar gegevens uitwisselen waarover zij beschikken in verband met de cyberrisico's en de cyberincidenten waarmee de exploitant wordt of kan worden geconfronteerd, met name de gegevens die zij van nationale of internationale autoriteiten of organisaties ontvangen of die in verband staan met het nationaal Cybernoodplan.

§2. De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling.

Hoofdstuk VI: Erkenningsprocedure

Artikel 18. Algemeen

§1. De exploitant van een nieuwe inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorieën Cyber-1 tot en met Cyber-4, vraagt aan het Agentschap de erkenning van het NCB-systeem door bij het Agentschap een NCB-dossier in te dienen waarin het ontwerp van het genoemde systeem wordt gedocumenteerd.

§5. L'Agence peut adopter des recommandations ou un règlement technique concernant les modalités des tests et le contenu minimal du rapport.

Article 16. Notification des cyber-incidents

§1^{er}. L'exploitant notifie les cyber-incidents à l'Agence et au CCB.

§2. L'Agence peut formuler des recommandations et adopter un règlement technique concernant les modalités de la notification à l'Agence des cyber-incidents et les informations à inclure dans cette notification.

Chapitre V : Echange de données

Article 17. Echange des données entre l'Agence et le CCB concernant les cyber-risques et cyber-incidents auxquels l'exploitant est ou peut être confronté

§1^{er}. L'Agence et le CCB peuvent s'échanger les données dont ils disposent concernant les cyber-risques et les cyber-incidents auxquels l'exploitant est ou peut être confronté, en particulier les données reçues d'autorités ou d'organisations nationales ou internationales ou liées au plan national d'urgence cybernétique.

§2. Cet échange d'informations se limite à ce qui est pertinent et proportionné à l'objectif de cet échange.

Chapitre VI : Procédure d'agrément

Article 18. Général

§1^{er}. L'exploitant d'un nouvel établissement dont les réseaux et des systèmes d'information sont classés dans les catégories Cyber-1 à Cyber-4 sollicite auprès de l'Agence l'agrément du système de CSN en introduisant auprès d'elle un dossier de CSN qui documente ledit projet de système.

§2. Wanneer de exploitant in zijn inrichting meerdere van elkaar onafhankelijke netwerk- en informatiesystemen heeft die ingedeeld zijn in verschillende categorieën moet het NCB-dossier de gevraagde informatie voor elk van de onafhankelijke netwerk- en informatiesystemen bevatten.

§3. Het NCB-dossier bevat ten minste de volgende informatie:

- de indeling in categorieën van de netwerk- en informatiesystemen van de inrichting van de exploitant;
- het toegekende beveiligingsniveau van de netwerk- en informatiesystemen;
- het resultaat van een zelfevaluatie van het ontwerp NCB-systeem om aan te tonen dat het voldoet aan de verplichtingen van artikel 6, §1;
- een actieplan om het ontwerp van NCB-systeem uit te voeren.

§4. Het Agentschap kan aanbevelingen of een technisch reglement opstellen dat de inhoud en de modaliteiten voor het opstellen en het versturen aan het Agentschap van het NCB-dossier verder preciseert.

Artikel 19. Erkenningsprocedure van het NCB-systeem van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-1 of Cyber-2

§1. De exploitant van een nieuwe nucleaire installatie waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-1 of Cyber-2 dient het NCB-dossier gelijktijdig in met de aanvraag tot het bekomen van de erkenning van het fysiek beveiligingssysteem van een nucleaire installatie volgens de bepalingen van artikel 8, §1, van het KB fysieke beveiliging.

De exploitant van een nieuw vervoerbedrijf voor kernmateriaal dat transporten zal uitvoeren ingedeeld in groep A of B volgens de bepalingen van artikel 3 van het KB categorisering en waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie cyber-1 of cyber-2, dient het NCB-dossier gelijktijdig in met de aanvraag tot het

§2. Lorsque l'exploitant dispose dans son établissement de plusieurs réseaux et systèmes d'information indépendants les uns des autres et qui sont classés dans des catégories différentes, le dossier de CSN doit contenir les informations demandées pour chaque réseau et système d'information indépendant.

§3. Le dossier de CSN contient au moins les informations suivantes :

- la catégorisation des réseaux et des systèmes d'information de l'établissement de l'exploitant ;
- le niveau de sécurité attribué aux réseaux et systèmes d'information ;
- le résultat d'une auto-évaluation du projet de système de CSN s'attachant à montrer qu'il satisfait aux obligations de l'article 6, §1^{er} ;
- un plan d'action pour mettre en œuvre le projet du système de CSN.

§4. L'Agence peut adopter un règlement technique ou des recommandations précisant le contenu et les modalités d'établissement et de soumission à l'Agence du dossier de CSN.

Article 19. Procédure d'agrément du système de CSN d'un établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-1 ou Cyber-2

§1^{er}. L'exploitant de la nouvelle installation nucléaire dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-1 ou Cyber-2 soumet le dossier de CSN en même temps que la demande d'obtention de l'agrément du système de protection physique de l'installation nucléaire telle qu'elle est visée à l'article 8, §1^{er}, de l'AR protection physique.

L'exploitant d'une nouvelle entreprise de transport de matières nucléaires qui exécutera des transports de groupe A ou B suivant les dispositions de l'article 3 de l'AR catégorisation et dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-1 ou Cyber-2 soumet le dossier de CSN en même temps que la demande d'obtention de

bekomen van de erkenning van algemeen beveiligingssysteem volgens de bepalingen van artikel 9 §1 van het KB fysieke beveiliging.

l'agrément du système générique de sécurité telle qu'elle est visée à l'article 9, §1^{er}, de l'AR protection physique.

§2. Zodra het Agentschap verklaart dat het door de exploitant ingediende NCB-dossier volledig is, zal het overgaan tot het onderzoek ten gronde ervan.

§2. Dès que l'Agence déclare complet le dossier de CSN introduit par l'exploitant, elle l'examine au fond.

§3. Bij een positieve beslissing van het Agentschap wordt de goedkeuring van het NCB-dossier, al naargelang het geval, gelijktijdig afgeleverd met het advies van het Agentschap over het ontwerp van fysiek beveiligingssysteem zoals voorzien in artikel 8,§3 van KB fysieke beveiliging of op het ontwerp van het algemeen beveiligingssysteem zoals voorzien in artikel 9,§3 van KB fysieke beveiliging B.

§3. En cas de décision positive de l'Agence, l'approbation du dossier de CSN est délivrée en même temps que l'avis de l'Agence sur le projet de système de protection physique prévu par l'article 8, §3, de l'AR protection physique ou sur le projet de système générique de sécurité prévu par l'article 9, §3, l'AR protection physique, selon le cas.

§4. Na de goedkeuring van het NCB-dossier voert de exploitant het NCB-systeem uit.

§4. Une fois approuvé le dossier de CSN, l'exploitant met en œuvre le système de CSN.

§5. Het NCB-systeem moet operationeel zijn ten laatste op het moment van het einde van de uitvoering van het ontwerp van fysiek beveiligingssysteem of het ontwerp van het algemeen beveiligingssysteem.

§5. Le système de CSN est mis en œuvre au plus tard à la fin de l'exécution du projet de système de protection physique ou du projet de système générique de sécurité.

§6. Wanneer het NCB-systeem is uitgevoerd, laat de exploitant het systeem extern auditen door een conformiteitsbeoordelingsinstantie die geaccrediteerd is door een nationale accreditatie-instantie en erkend werd door het CCB. De exploitant maakt de resultaten van deze audit over aan het Agentschap.

§6. Une fois le système de CSN mis en œuvre, l'exploitant le soumet à un audit externe réalisé par un organisme d'évaluation de la conformité accrédité par un organisme national d'accréditation et agréé par le CCB. L'exploitant transmet à l'Agence les résultats de cet audit.

§7. Wanneer het Agentschap vaststelt dat het NCB-systeem voldoet aan de vereisten van artikel 6, erkent het dit NCB-systeem en brengt het de exploitant op de hoogte van deze beslissing.

§7. Une fois que l'Agence estime que le système de CSN satisfait aux exigences de l'article 6, elle agréee ce système et elle informe l'exploitant de cette décision.

§8. In geval van een gehele of gedeeltelijke weigering tot erkenning, motiveert het Agentschap zijn beslissing.

§8. En cas de refus de délivrer, en tout ou en partie, l'agrément sollicité, l'Agence motive sa décision.

§9. De intentie tot gehele of gedeeltelijke weigering wordt aan de exploitant medegedeeld. Hierbij wordt verduidelijkt dat hij het recht heeft om binnen de dertig kalenderdagen vanaf de betekening van het voornemen tot gehele of gedeeltelijke weigering gehoord te worden. De exploitant wordt in voorkomend geval gehoord door het Agentschap dat bij zijn beslissing rekening houdt met de bijkomende elementen die worden verstrekt. De exploitant kan er tevens voor opteren om zijn opmerkingen louter schriftelijk aan het Agentschap te bezorgen binnen de voormelde dertig kalenderdagen. Wanneer de exploitant geen gebruik maakt van zijn recht om gehoord te worden of geen schriftelijke opmerkingen bezorgt, weigert het Agentschap ambtshalve de erkenning voor wat betreft het deel van de erkenning waarop de intentie tot weigering betrekking had.

§10. Indien de beslissing van het Agentschap, vermeld in §8, door de exploitant wordt betwist, kan deze een beroep indienen bij de Minister waarvan het Agentschap afhangt binnen de 3 maanden die volgen op de kennisgeving van de beslissing van het Agentschap. Deze treft alle nodige maatregelen om het geschil te beslechten en doet in laatste instantie een uitspraak over de erkenningsaanvraag.

§11. Het Agentschap kan een technisch reglement of aanbevelingen opstellen betreffende de modaliteiten van deze erkenningsprocedure.

Artikel 20. Erkenningsprocedure van het NCB-systeem van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-3

§1. De exploitant van een nieuwe inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-3 dient het NCB-dossier gelijktijdig in met het beveiligingsplan dat in toepassing van het KB RAMAS moet ingediend worden.

§2. Zodra het Agentschap verklaart dat het door de exploitant ingediende NCB-dossier

§9. L'exploitant est informé de l'intention de refuser en tout ou en partie. Il lui est également précisé qu'il a le droit d'être entendu dans les trente jours calendriers suivant la notification de l'intention de refuser en tout ou en partie. Le cas échéant, l'exploitant est entendu par l'Agence qui rend sa décision en tenant compte des éléments complémentaires fournis. L'exploitant peut également choisir de transmettre ses observations à l'Agence par écrit uniquement dans le délai de trente jours calendriers susmentionné. Lorsque l'exploitant ne recourt pas à son droit d'être entendu ou ne fournit pas d'observations écrites, l'Agence refuse d'office l'agrément pour la partie de l'agrément visée par l'intention de refus.

§10. Si l'exploitant conteste la décision de l'Agence mentionnée au §8, il peut introduire un recours auprès du Ministre dont relève l'Agence dans les 3 mois qui suivent la notification de la décision. Celui-ci prend toutes les mesures requises pour régler le différend et statue en dernier ressort sur la demande d'agrément.

§11. L'Agence peut adopter un règlement technique ou des recommandations concernant les modalités d'établissement de cette procédure d'agrément.

Article 20. Procédure d'agrément du système de CSN d'un établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-3

§1^{er}. L'exploitant d'un nouvel établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-3 soumet le dossier de CSN en même temps que le plan de sécurité qui doit être soumis en application de l'AR RAMAS.

§2. Dès que l'Agence déclare complet le dossier de CSN introduit par l'exploitant, elle l'examine au fond.

volledig is, zal het overgaan tot het onderzoek ten gronde ervan.

§3. Bij een positieve beslissing van het Agentschap wordt de goedkeuring van het NCB-dossier gelijktijdig afgeleverd met de goedkeuring van het beveiligingsplan voorzien in het KB RAMAS.

§4. Na de goedkeuring van het NCB-dossier voert de exploitant het NCB-systeem uit.

§5. Het NCB-systeem moet operationeel zijn ten laatste op het ogenblik van de in bedrijfsstelling zoals voorzien in artikel 15 van het algemeen reglement.

§6. Wanneer het NCB-systeem is uitgevoerd, laat de exploitant het systeem extern auditen door een conformiteitsbeoordelingsinstantie die geaccrediteerd is door een nationale accreditatie-instantie en erkend werd door het CCB. De exploitant maakt de resultaten van deze audit over aan het Agentschap.

§7. Wanneer het Agentschap vaststelt dat het NCB-systeem voldoet aan de vereisten van artikel 6, erkent het dit NCB-systeem en brengt het de exploitant op de hoogte van deze beslissing.

§8. In geval van een gehele of gedeeltelijke weigering tot erkenning, motiveert het Agentschap zijn beslissing.

§3. En cas de décision positive de l'Agence, l'approbation du dossier de CSN est délivrée en même temps que l'approbation du plan de sécurité radiologique prévue par l'AR RAMAS.

§4. Une fois approuvé le dossier de CSN, l'exploitant met en œuvre le système de CSN.

§5. Le système de CSN doit être mis en œuvre au plus tard au moment de la mise en exploitation visée à l'article 15 du règlement général.

§6. Une fois le système de CSN mis en œuvre, l'exploitant le soumet à un audit externe réalisé par un organisme d'évaluation de la conformité accrédité par un organisme national d'accréditation et agréé par le CCB. L'exploitant transmet à l'Agence les résultats de cet audit.

§7. Une fois que l'Agence estime que le système de CSN satisfait aux exigences de l'article 6, elle agréee ce système et elle informe l'exploitant de cette décision.

§8. En cas de refus de délivrer, en tout ou en partie, l'agrément sollicité, l'Agence motive sa décision.

§9. L'exploitant est informé de l'intention de refuser en tout ou en partie. Il lui est également précisé qu'il a le droit d'être entendu dans les trente jours calendriers suivant la notification de l'intention de refuser en tout ou en partie. Le cas échéant, l'exploitant est entendu par l'Agence qui rend sa décision en tenant compte des éléments complémentaires fournis. L'exploitant peut également choisir de transmettre ses observations à l'Agence par écrit uniquement dans le délai de trente jours calendriers susmentionné. Lorsque l'exploitant ne recourt pas à son droit d'être entendu ou ne fournit pas d'observations écrites, l'Agence refuse d'office l'agrément pour la partie de l'agrément visée par l'intention de refus.

§9. De intentie tot gehele of gedeeltelijke weigering wordt aan de exploitant medegedeeld. Hierbij wordt verduidelijkt dat hij het recht heeft om binnen de dertig kalenderdagen vanaf de betekening van het voornemen tot gehele of gedeeltelijke weigering gehoord te worden. De exploitant wordt in voorkomend geval gehoord door het Agentschap dat bij zijn beslissing rekening houdt met de bijkomende elementen die worden verstrekt. De exploitant kan er tevens voor opteren om zijn opmerkingen louter schriftelijk aan het Agentschap te bezorgen binnen de voormelde dertig kalenderdagen. Wanneer de exploitant geen gebruik maakt van zijn recht om gehoord te worden of geen schriftelijke opmerkingen bezorgt, weigert het Agentschap ambtshalve de erkenning voor wat betreft het deel van de erkenning waarop de intentie tot weigering betrekking had.

§10. Indien beslissing van het Agentschap vermeld in §8 door de exploitant wordt betwist, kan deze een beroep indienen bij de Minister waarvan het Agentschap afhangt binnen de 3 maanden die volgen op de kennisgeving van de beslissing. Deze treft alle nodige maatregelen om het geschil te beslechten en doet in laatste instantie een uitspraak over de erkenningsaanvraag.

§11. Het Agentschap kan een technisch reglement of aanbevelingen opstellen betreffende de modaliteiten van deze erkenningsprocedure.

Artikel 21. Erkenningsprocedure van het NCB-systeem van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-4

§1. De exploitant van een nieuwe inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-4 dient het NCB-dossier in gelijktijdig met het beveiligingsplan dat in toepassing van het KB RAMAS moet ingediend worden.

De exploitant van een nieuwe inrichting voor bovengrondse berging van radioactief afval waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-4 dient het NCB-dossier in te dienen gelijktijdig met het

§10. Si l'exploitant conteste la décision de l'Agence mentionnée au §8, il peut introduire un recours auprès du Ministre dont relève l'Agence dans les 3 mois qui suivent la notification de la décision. Celui-ci prend toutes les mesures requises pour régler le différend et statue en dernier ressort sur la demande d'agrément.

§11. L'Agence peut adopter un règlement technique ou des recommandations concernant les modalités d'établissement de cette procédure d'agrément.

Article 21. Procédure d'agrément du système de CSN d'un établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-4

§1^{er}. L'exploitant d'un nouvel établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-4 soumet le dossier de CSN en même temps que le plan de sécurité qui doit être soumis en application de l'AR RAMAS.

L'exploitant d'un nouvel établissement de stockage en surface dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-4 soumet le dossier de CSN en même temps que le plan de sécurité pour

beveiligingsplan voor de exploitatiefase dat in toepassing van het KB berging moet ingediend worden.

§2. Zodra het Agentschap verklaart dat het door de exploitant ingediende NCB-dossier volledig is, zal het overgaan tot het onderzoek ten gronde ervan.

§3. Bij een positieve beslissing van het Agentschap wordt de goedkeuring van het NCB-dossier gelijktijdig afgeleverd, met de goedkeuring van het beveiligingsplan voorzien in het KB RAMAS of met de goedkeuring van het beveiligingsplan voor de exploitatiefase voorzien in het KB berging, al naargelang het geval.

§4. Na de goedkeuring van het NCB-dossier voert de exploitant het NCB-systeem uit.

§5. Het NCB-systeem moet operationeel zijn, al naargelang het geval, ten laatste op het ogenblik van de in bedrijfsstelling zoals voorzien in artikel 15 van het algemeen reglement of op het ogenblik van de oplevering van de exploitatiefase van de inrichting voor bovengrondse berging van radioactief afval conform artikel 24 van het KB berging.

§6. Wanneer het NCB-systeem is uitgevoerd, laat de exploitant het systeem extern auditen. De exploitant maakt de resultaten van deze audit over aan het Agentschap.

§7. Wanneer het Agentschap vaststelt dat het NCB-systeem voldoet aan de vereisten van artikel 6, erkent het dit NCB-systeem en brengt het de exploitant op de hoogte van deze beslissing.

§8. In geval van een gehele of gedeeltelijke weigering tot erkenning, motiveert het Agentschap zijn beslissing.

la phase d'exploitation qui doit être soumis en application de l'AR stockage.

§2. Dès que l'Agence déclare complet le dossier de CSN introduit par l'exploitant, elle l'examine au fond.

§3. En cas de décision positive de l'Agence, l'approbation du dossier de CSN est délivrée, selon le cas, en même temps que l'approbation du plan de sécurité prévu par l'AR RAMAS ou en même temps que l'approbation du plan de sécurité pour la phase d'exploitation prévue par l'AR stockage.

§4. Une fois approuvé le dossier de CSN, l'exploitant met en œuvre le système de CSN.

§5. Le système de CSN doit être mis en œuvre au plus tard, selon le cas, au moment de la mise en exploitation visée à l'article 15 du règlement général ou au moment de la réception de la phase d'exploitation de d'établissement de stockage en surface conformément à l'article 24 de l'AR stockage

§6. Une fois le système de CSN mis en œuvre, l'exploitant le soumet à un audit externe. L'exploitant transmet à l'Agence les résultats de cet audit.

§7. Une fois que l'Agence estime que le système de CSN satisfait aux exigences de l'article 6, elle agréé ce système et elle informe l'exploitant de cette décision.

§8. En cas de refus de délivrer, en tout ou en partie, l'agrément sollicité, l'Agence motive sa décision.

§9. De intentie tot gehele of gedeeltelijke weigering wordt aan de exploitant medegedeeld. Hierbij wordt verduidelijkt dat hij het recht heeft om binnen de dertig kalenderdagen vanaf de betekening van het voornemen tot gehele of gedeeltelijke weigering gehoord te worden. De exploitant wordt in voorkomend geval gehoord door het Agentschap dat bij zijn beslissing rekening houdt met de bijkomende elementen die worden verstrekt. De exploitant kan er tevens voor opteren om zijn opmerkingen louter schriftelijk aan het Agentschap te bezorgen binnen de voormelde dertig kalenderdagen. Wanneer de exploitant geen gebruik maakt van zijn recht om gehoord te worden of geen schriftelijke opmerkingen bezorgt, weigert het Agentschap ambtshalve de erkenning voor wat betreft het deel van de erkenning waarop de intentie tot weigering betrekking had.

§10. Indien de beslissing van het Agentschap door de exploitant vermeld in §8 wordt betwist, kan deze een beroep indienen bij de Minister waarvan het Agentschap afhangt binnen de 3 maanden die volgen op de kennisgeving van de beslissing. Deze treft alle nodige maatregelen om het geschil te beslechten en doet in laatste instantie een uitspraak over de erkenningsaanvraag.

§11. Het Agentschap kan een technisch reglement of aanbevelingen opstellen betreffende de modaliteiten van deze erkenningsprocedure.

Artikel 22. Wijzigingen in het NCB-systeem

§1. Elke wijziging aan de inrichting of aan de netwerk- en informatiesystemen die als gevolg een wijziging veroorzaken van de categorie waarin deze netwerk- en informatiesystemen werden ingedeeld, moet het voorwerp uitmaken van een wijziging in het NCB-systeem.

§2. De wijziging van het NCB-systeem moet vooraf door het Agentschap worden erkend volgens de modaliteiten voorzien in dit hoofdstuk. Het Agentschap kan na consultatie van de exploitant de termijnen bepalen voor

§9. L'exploitant est informé de l'intention de refuser en tout ou en partie. Il lui est également précisé qu'il a le droit d'être entendu dans les trente jours calendriers suivant la notification de l'intention de refuser en tout ou en partie. Le cas échéant, l'exploitant est entendu par l'Agence qui rend sa décision en tenant compte des éléments complémentaires fournis. L'exploitant peut également choisir de transmettre ses observations à l'Agence par écrit uniquement dans le délai de trente jours calendriers susmentionné. Lorsque l'exploitant ne recourt pas à son droit d'être entendu ou ne fournit pas d'observations écrites, l'Agence refuse d'office l'agrément pour la partie de l'agrément visée par l'intention de refus.

§10. Si l'exploitant conteste la décision de l'Agence mentionnée au §8, il peut introduire un recours auprès du Ministre dont relève l'Agence dans les 3 mois qui suivent la notification de la décision. Celui-ci prend toutes les mesures requises pour régler le différend et statue en dernier ressort sur la demande d'agrément.

§11. L'Agence peut adopter un règlement technique ou des recommandations concernant les modalités d'établissement de cette procédure d'agrément.

Article 22. Modifications dans le système de CSN

§1^{er}. Toute modification apportée à l'établissement ou à ses réseaux et systèmes d'information qui entraîne un changement de la catégorie dans laquelle ceux-ci ont été classés fait l'objet d'une modification du système de CSN.

§2. La modification du système de CSN est soumise à l'agrément préalable de l'Agence selon les modalités prévues au présent chapitre. L'Agence peut, après consultation de l'exploitant, déterminer les délais de

het uitvoeren van de wijzigingen van het NCB-systeem.

§3. Het Agentschap kan aanbevelingen of een technisch reglement opstellen betreffende de inhoud en de modaliteiten voor het opstellen en het versturen aan het Agentschap van het gewijzigde NCB-systeem.

Hoofdstuk VII: Verificatie

Artikel 23. Audits

§1. De exploitant van een inrichting, waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorieën Cyber-1 tot Cyber-3, voert, na de erkenning van het NCB-systeem, elk jaar een interne audit uit van de werking van het NCB-systeem.

§2. De exploitant van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-1, laat, na de erkenning van het NCB-systeem, elke drie jaar de werking van het NCB-systeem extern auditeren door een conformiteitsbeoordelingsinstantie die geaccrediteerd is door een nationale accreditatie-instantie en erkend werd door het CCB.

In de twee jaren volgend op de externe audit voorzien in artikel 19, §6, laat de exploitant jaarlijks een opvolgingsaudit uitvoeren door een conformiteitsbeoordelingsinstantie die geaccrediteerd is door een nationale accreditatie-instantie en erkend werd door het CCB.

§3. De exploitant van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorieën Cyber-2 of Cyber-3, laat, na de erkenning van het NCB-systeem, elke drie jaar de werking van het NCB-systeem extern auditeren door een conformiteitsbeoordelingsinstantie die geaccrediteerd is door een nationale accreditatie-instantie en erkend werd door het CCB.

§4. De exploitant van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in de categorie Cyber-4, voert, na de erkenning van het NCB-systeem, elke twee

l'exécution des modifications du système de CSN.

§3. L'Agence peut adopter un règlement technique ou des recommandations concernant le contenu et les modalités d'établissement et de soumission à l'Agence du système de CSN modifié.

Chapitre VII : Vérification

Article 23. Audits

§1. L'exploitant de l'établissement dont les réseaux et systèmes d'information sont classés dans les catégories Cyber-1 à Cyber-3 procède, chaque année après l'agrément du système de CSN, à un audit interne du fonctionnement de son système de CSN.

§2. L'exploitant de l'établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-1 soumet, tous les trois ans après l'agrément de son système de CSN, le fonctionnement de son système de CSN à un audit externe réalisé par un organisme d'évaluation de la conformité accrédité par un organisme national d'accréditation et agréé par le CCB.

Dans les deux ans qui suivent l'audit externe prévu à l'article 19, §6, l'exploitant fait procéder chaque année à un audit de suivi par un organisme d'évaluation de la conformité accrédité par un organisme national d'accréditation et agréé par le CCB.

§3. Tous les trois ans après l'agrément du système de CSN, l'exploitant de l'établissement dont les réseaux et systèmes d'information sont classés dans les catégories Cyber-2 à Cyber-3 soumet le fonctionnement de son système de CSN à un audit externe réalisé par un organisme d'évaluation de la conformité accrédité par un organisme national d'accréditation et agréé par le CCB.

§4. L'exploitant de l'établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-4 procède tous les deux ans après l'agrément du

jaar een interne audit uit van de werking van het NCB-systeem.

§5. De exploitant van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in de categorie Cyber-4, laat, na de erkenning van het NCB-systeem, elke vijf jaar de werking van het NCB-systeem extern auditeren.

Hoofdstuk VIII: Technische reglementen

Artikel 24.

De technische reglementen die het Agentschap overeenkomstig de artikelen 12 § 2, 13 §2 en 14 §2, kan opstellen, zullen voornamelijk gebaseerd zijn op het referentiekader vermeld in artikel 4 van het KB ter uitvoering van de NIS2-wet, ze kunnen ook worden gebaseerd op internationaal aanvaarde technische normen en op de aanbevelingen van het Internationaal Atoomenergie Agentschap inzake nucleaire cyberbeveiliging.

De voorschriften van de technische reglementen zullen rekening houden met het te garanderen beveiligingsniveau.

Hoofdstuk IX: Overgangsmaatregelen

Artikel 25. Toepassingsgebied van dit hoofdstuk

Dit hoofdstuk is van toepassing op exploitanten die op het ogenblik van de inwerkingtreding van dit besluit vergund zijn in toepassing van artikel 7 of 8 van het algemeen reglement en op exploitanten die op het ogenblik van de inwerkingtreding van dit besluit, in toepassing van artikel 8 §1 van het KB fysieke beveiliging een erkend fysiek beveiligingssysteem ingericht hebben of een erkend generiek beveiligingssysteem in toepassing van artikel 9, §1 van hetzelfde besluit.

Artikel 26. Overgangsmaatregelen met betrekking tot het NCB-dossier

Het NCB-dossier voorzien in artikel 6, §3, bevat ten minste de volgende informatie:

système de CSN à un audit interne du fonctionnement de son système de CSN.

§5. Tous les cinq ans après l'agrément du système de CSN, l'exploitant de l'établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-4 soumet le fonctionnement de son système de CSN à un audit externe.

Chapitre VIII : Règlements techniques

Article 24.

Les règlements techniques que l'Agence peut adopter en vertu des articles 12 §2, 13 §2 et 14 §52, seront établis principalement à partir du cadre de référence mentionné à l'article 4 de l'AR d'exécution de la loi NIS2, ils pourront en outre être établis à partir de normes techniques internationalement reconnues ainsi qu'à partir des recommandations de l'Agence internationale de l'Energie atomique en matière de cybersécurité nucléaire.

Les prescriptions des règlements technique tiendront compte du niveau de sécurité à assurer.

Chapitre IX : Mesures transitoires

Article 25. Champ d'application du chapitre

Le présent chapitre s'applique aux exploitants autorisés en application des dispositions de l'article 7 ou 8 du règlement général au moment de l'entrée en vigueur du présent arrêté, ainsi qu'aux exploitants ayant mis en place, au moment de l'entrée en vigueur du présent arrêté, un système de protection physique agréé en application de l'article 8, §1^{er}, de l'AR protection physique ou un système générique de sécurité agréé en application de l'article 9, §1 du même arrêté.

Article 26. Mesures transitoires concernant le dossier de CSN

Le dossier de CSN prévu par l'article 6, §3, contient au moins les informations suivantes :

- de indeling in categorieën van de netwerk- en informatiesystemen aanwezig in de inrichting van de exploitant;
- het toegekende beveiligingsniveau aan deze netwerk- en informatiesystemen;
- het resultaat van een zelfevaluatie van het NCB-systeem om aan te tonen dat het voldoet aan de verplichtingen van artikel 6, §1;
- een door de afgevaardigde voor NCB goedgekeurd actieplan om, indien nodig, het NCB-systeem op het vereiste beveiligingsniveau te brengen.

- la catégorisation des réseaux et des systèmes d'information de l'établissement de l'exploitant ;
- le niveau de sécurité attribué aux réseaux et systèmes d'information ;
- le résultat d'une auto-évaluation du système de CSN s'attachant à montrer qu'il satisfait aux obligations de l'article 6, §1^{er} ;
- un plan d'action, approuvé par le délégué à la CSN pour mettre le système de CSN au niveau de sécurité requis, si nécessaire.

Artikel 27. Overgangsmaatregelen voor de erkenning van het NCB-systeem van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-4

De exploitant van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-4 dient, ten laatste 12 maanden na de inwerkingtreding van dit besluit, een NCB-dossier uit te werken.

De exploitant moet het NCB-systeem uitgevoerd hebben ten laatste 24 maanden na de inwerkingtreding van dit besluit.

Op het ogenblik dat het NCB-systeem is uitgevoerd en het NCB-systeem voldoet aan de vereisten van artikel 6, §1 tot §3, wordt het als erkend beschouwd.

Een kopie van het NCB-dossier is te allen tijde ter beschikking van het Agentschap en dient op het eerste verzoek te worden overgemaakt.

Article 27. Mesures transitoires pour l'agrément du système de CSN d'un établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-4

L'exploitant de l'établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-4 doit, au plus tard 12 mois après l'entrée en vigueur du présent arrêté, élaborer le dossier de CSN.

L'exploitant doit mettre le système de CSN en œuvre au plus tard 24 mois après l'entrée en vigueur du présent arrêté.

Une fois que le système de CSN est mis en œuvre, et qu'il satisfait aux exigences de l'article 6, §1 à §3, il est considéré agréé.

Une copie du dossier de CSN est toujours tenue à la disposition de l'Agence et doit lui être transmise à la première demande.

Artikel 28. Overgangsmaatregelen voor de erkenning van het NCB-systeem van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-1, Cyber-2 of Cyber-3

§1. De exploitant van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in categorie Cyber-1 of Cyber-2 of Cyber-3, dient zijn aanvraag tot erkenning in binnen de acht maanden die volgen op de inwerkingtreding van dit besluit.

§2. Zodra het Agentschap verklaart dat het door de exploitant ingediende NCB- dossier volledig is, beschikt het over vier maanden om

Article 28. Mesures transitoires pour l'agrément du système de CSN d'un établissement dont les réseaux et systèmes d'information sont classés dans les catégories Cyber-1, Cyber-2 ou Cyber-3

§1^{er}. L'exploitant de l'établissement dont les réseaux et systèmes d'information sont classés dans la catégorie Cyber-1, Cyber-2 ou Cyber-3 introduit la demande d'agrément du système de CNS dans les huit mois suivant l'entrée en vigueur du présent arrêté.

§2. Dès que l'Agence déclare complet le dossier de NCS introduit par l'exploitant, elle

over te gaan tot het onderzoek ervan en het goed te keuren.

§3. Na de goedkeuring dient de exploitant het NCB-systeem uit te voeren binnen een periode van maximaal drie jaar.

§4. Om het Agentschap toe te laten de uitvoering van het NCB-systeem op te volgen wordt de eerste drie jaar na de goedkeuring, het jaarverslag van de afgevaardigde voor NCB, voorzien in artikel 9, §11, jaarlijks en ten laatste op 1 maart aan het Agentschap overgemaakt. Het Agentschap evalueert de vooruitgang van de implementatie van het NCB-systeem via dit jaarverslag.

§5. Wanneer het NCB-systeem is uitgevoerd, laat de exploitant het systeem extern auditen door een conformiteitsbeoordelingsinstantie die geaccrediteerd is door een nationale accreditatie-instantie en erkend werd door het CCB. De exploitant maakt de resultaten van deze audit over aan het Agentschap.

§6. Wanneer het Agentschap vaststelt dat het NCB-systeem voldoet aan de vereisten van artikel 6, erkent het dit NCB-systeem binnen de 6 maanden en brengt het de exploitant op de hoogte van deze beslissing.

§7. In geval van een gehele of gedeeltelijke weigering tot erkenning, motiveert het Agentschap zijn beslissing.

§8. De intentie tot gehele of gedeeltelijke weigering wordt aan de exploitant medegedeeld. Hierbij wordt verduidelijkt dat hij het recht heeft om binnen de dertig kalenderdagen vanaf de betekening van het voornemen tot gehele of gedeeltelijke weigering gehoord te worden. De exploitant wordt in voorkomend geval gehoord door het Agentschap dat bij zijn beslissing rekening houdt met de bijkomende elementen die worden verstrekt. De exploitant kan er tevens voor opteren om zijn opmerkingen louter schriftelijk aan het Agentschap te bezorgen binnen de voormelde dertig kalenderdagen. Wanneer de exploitant geen gebruik maakt van zijn recht om gehoord te worden of geen schriftelijke opmerkingen bezorgt, weigert het

dispose de quatre mois pour l'examiner et pour l'approuver.

§3. Une fois approuvé, le système de CSN doit être mis en œuvre par l'exploitant dans un délai de trois ans maximum.

§4. Pour permettre à l'Agence de suivre la mise en œuvre du système de CSN, le rapport annuel du délégué à la CSN prévu à l'article 9, §11, est transmis chaque année à l'Agence au plus tard le 1^{er} mars de chacune des trois premières années suivant l'approbation. L'Agence évalue l'avancement de la mise en œuvre du système de CSN sur la base de ce rapport annuel.

§5. Une fois le système de CSN mis en œuvre, l'exploitant le soumet à un audit externe réalisé par un organisme d'évaluation de la conformité accrédité par un organisme national d'accréditation et agréé par le CCB. L'exploitant transmet à l'Agence les résultats de cet audit.

§6. Une fois que l'Agence estime que le système de CSN satisfait aux exigences de l'article 6, elle agréé dans les 6 mois ce système et elle informe l'exploitant de cette décision.

§7. En cas de refus de délivrer, en tout ou en partie, l'agrément sollicité, l'Agence motive sa décision.

§8. L'exploitant est informé de l'intention de refuser en tout ou en partie. Il lui est également précisé qu'il a le droit d'être entendu dans les trente jours calendriers suivant la notification de l'intention de refuser en tout ou en partie. Le cas échéant, l'exploitant est entendu par l'Agence qui rend sa décision en tenant compte des éléments complémentaires fournis. L'exploitant peut également choisir de transmettre ses observations à l'Agence par écrit uniquement dans le délai de trente jours calendriers susmentionné. Lorsque l'exploitant ne recourt pas à son droit d'être entendu ou ne fournit pas d'observations écrites, l'Agence refuse d'office l'agrément pour la partie de l'agrément visée par l'intention de refus.

Agentschap ambtshalve de erkenning voor wat betreft het deel van de erkenning waarop de intentie tot weigering betrekking had.

§9. Indien beslissing van het Agentschap vermeld in §7 door de exploitant wordt betwist, kan deze een beroep indienen bij de Minister waarvan het Agentschap afhangt, dit binnen de drie maanden die volgen op de kennisgeving van de beslissing van het Agentschap. De Minister beslist finaal over de erkenningsaanvraag.

Artikel 29. Overgangsbepalingen voor de aanstelling van de afgevaardigde voor Nucleaire Cyberbeveiliging

Binnen de drie maanden na de inwerkingtreding van dit besluit, dient de exploitant van een inrichting waarvan de netwerk- en informatiesystemen, volgens de bepalingen van artikel 3, ingedeeld zijn in categorie Cyber-1, Cyber-2, Cyber-3 en Cyber-4, de afgevaardigde voor nucleaire cyberbeveiliging aan te stellen en de aanvraag tot goedkeuring van de aanstelling voorzien in artikel 8, §3, van dit besluit aan het Agentschap over te maken.

Hoofdstuk X: Slotbepalingen

Artikel 30.

Dit besluit wordt aangehaald als: "koninklijk besluit betreffende de nucleaire cyberbeveiliging".

Artikel 31.

De Minister bevoegd voor Binnenlandse Zaken is belast met de uitvoering van dit besluit.

§9. Si l'exploitant conteste la décision de l'Agence mentionnée au §7, il peut introduire un recours auprès du ministre dont dépend l'Agence dans les trois mois suivant la notification de la décision de l'Agence. La décision finale sur la demande d'agrément appartient au ministre.

Article 29. Mesures transitoires pour la désignation du délégué à la cybersécurité nucléaire

Dans les trois mois suivant l'entrée en vigueur du présent arrêté, l'exploitant d'un établissement où les réseaux et systèmes d'information sont classés, selon les dispositions de l'article 3, dans la catégorie Cyber-1, Cyber-2, Cyber-3 ou Cyber-4, doit désigner le délégué à la cybersécurité nucléaire et transmettre à l'Agence la demande de l'approbation de la désignation visée à l'article 8, §3, du présent arrêté.

Chapitre X : Dispositions finales

Article 30.

Le présent arrêté est cité comme « l'arrêté royal relatif à la cybersécurité nucléaire ».

Article 31.

Le Ministre qui a l'Intérieur dans ses attributions est chargé de l'exécution du présent arrêté.

Hoofdstuk XI: Inwerkingtreding

Artikel 32.

Dit besluit treedt in werking op de eerste dag van de derde maand na de publicatie in het Belgisch staatsblad.

Gegeven te
op ...

Chapitre XI : Entrée en vigueur

Article 32.

Le présent arrêté entre en vigueur le premier jour du troisième mois qui suit celui de sa publication au Moniteur belge.

,
Donné à
le ...

Van Koningswege,

De Minister van Veiligheid en Binnenlandse
Zaken, belast met Beliris,

Par le Roi,

Le Ministre de la Sécurité et de l'Intérieur
également chargé de Beliris,



Bernard Quintin

**Federaal Agentschap voor Nucleaire
Controle**

Agence fédérale de Contrôle nucléaire

Koninklijk besluit tot uitvoering van artikel 17*sexies*, §1, van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

Arrêté royal portant exécution de l'article 17*sexies*, §1, de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

VERSLAG AAN DE KONING,

RAPPORT AU ROI,

Sire,

Sire,

Dit ontwerp van koninklijk besluit wordt genomen in uitvoering van artikel 17*sexies* §1 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, artikel aangenomen bij wet van 5 april 2019.

Le présent projet d'arrêté royal est pris en exécution de l'article 17*sexies*, §1, de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, article qui a été adopté par la loi du 5 avril 2019.

Dit ontwerp van koninklijk besluit regelt in het bijzonder één van de in §1 van artikel 17*sexies* voorziene vier machtigingen voor de Koning, namelijk die om de nucleaire cyberbeveiligingsmaatregelen te bepalen die aan de exploitanten worden opgelegd.

Le présent projet d'arrêté royal règle notamment l'une des quatre habilitations au Roi visées au § 1er de l'article 17*sexies*, celle qui habilite le Roi à déterminer les mesures de cybersécurité nucléaire imposées aux exploitants.

Er moet aan herinnerd worden dat de nucleaire cyberbeveiliging (hierna NCB), zoals gedefinieerd in artikel 1 van de wet van 15 april 1994, niet enkel de cyberbeveiliging in nucleaire installaties en inrichtingen betreft maar eveneens de cyberbeveiliging in de inrichtingen waar radioactieve stoffen aanwezig zijn alsook de cyberbeveiliging van nucleaire vervoerbedrijven en andere vervoerders van radioactieve stoffen. Er moet echter wel opgemerkt worden dat systemen die zich aan boord van voertuigen bevinden niet onder dit ontwerpbesluit vallen.

Il convient de rappeler ici que la cybersécurité nucléaire (ci-après CSN), telle qu'elle est définie à l'article 1ier de la loi du 15 avril 1994, comprend non seulement la cybersécurité dans les installations et établissements nucléaires, mais aussi la cybersécurité dans les établissements où des substances radioactives sont présentes, y compris ceux des entreprises de transport nucléaire et des autres transporteurs de substances radioactives.

Toutefois, il convient de noter que les systèmes situés à bord des véhicules ne sont pas couverts par ce projet d'arrêté.

Netwerk- en informatiesystemen hebben een essentiële plaats ingenomen in ons dagelijks leven door de snelle digitale

Les réseaux et systèmes d'information sont devenus des caractéristiques essentielles de notre vie quotidienne en raison de la

transformatie en de onderlinge verbondenheid binnen de samenleving. Die ontwikkeling heeft geleid tot een uitbreiding van het cyberdreigingslandschap, wat nieuwe uitdagingen met zich meebrengt, die een aangepaste, gecoördineerde en innovatieve respons vereisen.

Cyberbeveiliging is dus een specifieke aangelegenheid, met gemeenschappelijke en coherente algemene regels die van toepassing zijn op alle netwerk- en informatiesystemen, ongeacht het werkterrein waarop deze worden gebruikt.

De NIS2-richtlijn, omgezet door de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (hierna "NIS2-wet") sluit de nucleaire sector uit (de NIS2-wet is alleen van toepassing op "elementen van een nucleaire installatie die bestemd zijn voor de industriële productie van elektriciteit en die worden gebruikt voor de transmissie van elektriciteit", zie artikel 4, §4), en het is belangrijk dat ook een kader wordt gecreëerd voor de cyberbeveiliging van de nucleaire sector.

Exploitanten die radioactieve stoffen in hun bezit hebben, zijn niet noodzakelijk uitgesloten van het toepassingsgebied van de NIS2-wet en kunnen onder dit toepassingsgebied vallen afhankelijk van de activiteiten van de inrichtingen in kwestie. Indien dit niet het geval is, vallen ze, gezien de cyberdreigingen ook alomtegenwoordig zijn, onder de maatregelen van dit ontwerpbesluit en zijn er cyberbeveiligingsmaatregelen nodig om deze het hoofd te bieden.

Het doel van dit ontwerpbesluit is om zo nauw mogelijk aan te sluiten bij de bepalingen die voorzien zijn in de NIS2-wet. Daarom is de samenwerking met het CCB belangrijk. Er zal ook gebruik gemaakt worden van de reeds bestaande aanbevelingen die het CCB heeft opgesteld zoals het referentiekader (het CyberFundamentals framework) waarnaar

transformation numérique rapide et de l'interconnexion de la société.

Cette évolution a conduit à une expansion du paysage des cybermenaces et à l'émergence de nouveaux défis, qui nécessitent des réponses adaptées, coordonnées et novatrices.

La cybersécurité constitue ainsi une matière propre, avec des règles générales communes et cohérentes applicables à tous les réseaux et systèmes d'information, indépendamment du domaine d'activités dans lequel ceux-ci sont utilisés.

La directive NIS2, transposée par la loi du 26 avril 2024 instituant un cadre pour la cybersécurité des réseaux et systèmes d'information d'intérêt général pour la sécurité publique (ci-après "loi NIS2") ne s'applique pas au secteur nucléaire (la loi NIS2 ne s'applique qu'"aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.", voir son article 4, §4), et il est important qu'un cadre soit créé pour la cybersécurité du secteur nucléaire.

Les exploitants qui sont en possession, de substances radioactives ne sont pas nécessairement exclus du champ d'application de la loi NIS2 et peuvent relever de son champ d'application selon les activités des établissements considérés. Si ce n'est pas le cas, ils sont couverts par les mesures de ce projet d'arrêté, étant donné que les cybermenaces sont omniprésentes et que des mesures de cybersécurité doivent être prises contre elles.

Le but de ce projet d'arrêté est de s'aligner le plus possible avec les dispositions de la loi NIS2.

C'est pourquoi la coopération avec le CCB est importante. Il sera également fait usage des recommandations existantes élaborées par le CCB, comme le cadre de référence (le CyberFundamentals framework) auquel il sera fait directement référence via les

er via de technische reglementen die dit ontwerpbesluit zullen begeleiden, direct verwezen zal worden.

Dit ontwerpbesluit moet ook gezien worden als een aanvulling op de reeds bestaande regelgevingen voor de fysieke beveiliging van kernmaterialen enerzijds en de beveiliging van radioactieve stoffen anderzijds, waarbij de beveiligingssystemen aangevuld worden met een "cyberbeveiligingscomponent".

ARTIKELSGEWIJZE TOELICHTING

Artikel 1 bevat de definities van een aantal begrippen die in het ontwerp van koninklijk besluit worden gebruikt. Er worden in het besluit een aantal begrippen gebruikt die reeds gedefinieerd zijn in ofwel de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle (wet van 15 april 1994) of in het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen de gevaren van ioniserende stralingen (algemeen reglement). Als er naar het Agentschap verwezen worden is dat het Federaal Agentschap voor Nucleaire Controle opgericht door de Wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

Dit artikel moet eveneens samen gelezen worden met de bestaande wettelijke definities zoals deze van "netwerk- en informatiesysteem", "cyberincident" en "cyberrisico" (die overeenkomen met de definities in de NIS2-wet), waarnaar verwezen wordt. De definities van "nucleaire cyberbeveiliging" en "nucleaire cyberbeveiligingsmaatregelen" zijn opgenomen in artikel 1 van de wet van 15 april 1994. Hieruit volgt dat de nucleaire cyberbeveiliging kan worden opgevat als het vermogen van de netwerken en

règlements techniques qui accompagneront ce projet d'arrêté.

Ce projet d'arrêté doit également être considéré comme complément aux réglementations existantes sur la protection physique des matières nucléaires d'une part et sur la sécurité des substances radioactives d'autre part, dont les systèmes de sécurité doivent être complétés par un "volet portant sur la cybersécurité".

COMMENTAIRE DES ARTICLES

L'article 1^{er} contient les définitions de plusieurs termes utilisés dans le projet d'arrêté royal. L'arrêté utilise un certain nombre de termes qui ont déjà été définis soit dans la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire (Loi du 15 avril 1994) soit dans l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants (règlement général). Lorsque l'on fait référence à l'Agence, il s'agit de l'Agence fédérale de Contrôle nucléaire, établie par la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

Cet article également doit être lu conjointement avec les définitions légales existantes, telles que celles de « réseau et système d'information », de « cyberincident » et de « cyber-risque » (qui correspondent d'ailleurs aux définitions de la loi NIS2), auxquelles il est renvoyé. Les définitions de « cybersécurité nucléaire » et de « mesures de cybersécurité nucléaire » figurent à l'article 1^{er} de la loi du 15 avril 1994. Il en découle que la cybersécurité nucléaire peut être comprise comme le fait, pour les réseaux et systèmes d'information

informatiesystemen van de betrokken installaties en inrichtingen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens en de daaraan gerelateerde diensten die via deze netwerken en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen.

Er werd ook een nieuwe definitie van exploitant en inrichting toegevoegd om rekening te houden met het toepassingsgebied. Deze definitie omvat meer ondernemingen dan deze die in de Wet van 15 april 1994 of in het algemeen reglement zijn opgenomen.

Een exploitant in dit ontwerpbesluit omvat de exploitanten gedefinieerd in de wet van 15 april 1994 en in het algemeen reglement maar omvat ook expliciet een exploitant van een nucleaire installatie en de vervoerbedrijven van kernmaterialen, de definitie van inrichting werd aangepast in dezelfde zin als deze van exploitant.

Artikel 2 preciseert welke de netwerk- en informatiesystemen van installaties en inrichtingen zijn die tot het toepassingsgebied van dit ontwerpbesluit betreffende de nucleaire cyberbeveiliging behoren.

De netwerk- en informatiesystemen die zich bevinden in inrichtingen van de Belgische krijgsmacht vallen niet onder het toepassingsgebied van dit ontwerpbesluit. Dit ontwerp is niet van toepassing op de netwerk- en informatiesystemen in inrichtingen die enkel toestellen bevatten die ioniserende stralingen uitzenden die niet afkomstig zijn van radioactieve stoffen gezien de afwezigheid van een normatief kader betreffende de fysieke beveiliging van deze toestellen.

In dit artikel wordt eveneens bepaald dat de netwerk- en informatiesystemen die onder het toepassingsgebied van dit ontwerp vallen maar ook onder dat van de NIS2-wet, geacht worden onherroepelijk te voldoen aan de verplichtingen van dit ontwerpbesluit, inclusief de verplichtingen

des installations et des établissements visés, de résister avec un niveau de fiabilité donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.

Des définitions de l'exploitant et de l'établissement propres au présent projet ont également été ajoutées, pour refléter le champ d'application. Ces définitions couvrent davantage d'entreprises que celles figurant dans la loi du 15 avril 1994 ou dans le règlement général. Un exploitant dans ce projet d'arrêté couvre la notion d'exploitant définie dans la loi du 15 avril 1994 et dans le règlement général mais aussi explicitement celle de l'exploitant d'une installation nucléaire et d'une entreprise de transport des matières nucléaires. La définition d'établissement est adaptée de la même manière que la définition d'exploitant.

L'article 2 précise quels sont les réseaux et systèmes d'information des installations et établissements qui relèvent du champ d'application de cet arrêté sur la cybersécurité nucléaire en projet.

Le réseau et les systèmes d'information situés dans les établissements des forces armées belges n'entrent pas dans le champ d'application de ce projet d'arrêté, .

Le projet ne s'applique pas aux réseaux et systèmes d'information des établissements qui abritent uniquement des appareils émettant des rayonnements ionisants ne provenant pas de substances radioactives étant donné l'absence d'un cadre normatif sur la protection physique de ces appareils.

Cet article dispose également que les réseaux et systèmes d'information qui relèvent du champ d'application du présent projet mais aussi de celui de la loi NIS2 sont irréfragablement présumés satisfaire aux obligations du présent projet d'arrêté, y compris les obligations relatives à l'agrément

met betrekking tot de erkenning door het Federaal Agentschap voor Nucleaire Controle (hierna het Agentschap). De cyberbeveiliging van deze netwerk- en informatiesystemen moet gebeuren conform de NIS2-wet.

De uitzondering hierop zijn de netwerk- en informatiesystemen die geïntegreerd zijn in deze van een andere inrichting die onder het toepassingsgebied van dit ontwerpbesluit vallen, wat wil zeggen dat in dit geval de netwerk- en informatiesystemen moeten voldoen aan de bepalingen van dit ontwerpbesluit.

Het toepassingsgebied betreft alle soorten van systemen, zowel de systemen die instaan voor de informatietechnologie (IT) als deze voor de operationele technologie (OT) en IOT-systemen (Internet of Things). IT omvat alle technologieën die gebruikt worden om informatie te verzamelen, op te slaan, te verwerken en te communiceren, zoals vb.: computers, software, besturingssystemen, netwerken, databases, websites, servers, laptops, printers, scanners. OT omvat de technologieën die worden gebruikt om industriële processen te besturen en te monitoren. OT is de algemene noemer voor systemen die instaan voor bewaking en besturing (SCADA), Distributiecontrolesystemen (DCS), en Programmable Logic Controllers (PLC's). IoT staat voor "Internet of Things". Het is een netwerk van toestellen voor dagelijks gebruik die met elkaar verbonden zijn via internet. Deze apparaten kunnen data verzamelen en versturen en inzichtelijk maken op een smartphone, of ander draagbaar toestel. De verzameling van data zal voornamelijk door cloudapplicaties gebeuren. Voorbeelden hiervan zijn een slimme thermostaat die de temperatuur kan regelen, slimme verlichting, sensoren die de uitlaat in schoorstenen monitoren, sensoren op apparaten voor onderhoudsplanning, ...

Artikel 3 voorziet de indeling in categorieën van voormelde netwerk- en

par l'Agence fédérale de Contrôle nucléaire (ci-après l'Agence). La cybersécurité de ces réseaux et systèmes d'information doit donc être assurée conformément à la loi NIS2, Font exception à cette règle les réseaux et systèmes d'information qui sont intégrés dans les réseaux et systèmes régis par ce projet d'arrêté mais relevant d'un autre établissement; autrement dit, dans ce cas, ces réseaux et systèmes d'information doivent se conformer aux dispositions du présent arrêté.

Le champ d'application concerne tous les types de systèmes, y compris les systèmes de technologie de l'information (IT), les systèmes de technologie opérationnelle (OT) et les systèmes IOT (de l'Internet of Things). Les IT comprennent toutes les technologies utilisées pour collecter, stocker, traiter et communiquer des informations, par exemple : les ordinateurs, les logiciels, les systèmes d'exploitation, les réseaux, les bases de données, les sites web, les serveurs, les ordinateurs portables, les imprimantes, les scanners. L'OT comprend les technologies utilisées pour contrôler et surveiller les processus industriels. OT est le dénominateur général des systèmes responsables de la surveillance et du contrôle (SCADA), des systèmes de contrôle de la distribution (DCS) et des contrôleurs logiques programmables (PLC). IoT signifie « Internet of Things ». Il s'agit d'un réseau d'appareils d'usage courant connectés entre eux via l'internet. Ces appareils peuvent collecter et envoyer des données et les afficher sur un smartphone ou un autre appareil portable, la collecte des données étant principalement assurée par des applications en nuage. Parmi les exemples, citons un thermostat intelligent qui peut contrôler la température, un éclairage intelligent, des capteurs qui surveillent les gaz d'échappement dans les cheminées, des capteurs sur les appareils pour la planification de la maintenance, ...

L'article 3 prévoit la répartition en catégories des réseaux et systèmes

informatiesystemen op basis van de kritieke aard van die systemen. De criticiteit die in aanmerking moet worden genomen, houdt ook rekening met de mogelijke gevolgen van de compromittering van de systemen en netwerken op de nucleaire en radiologische veiligheid en beveiliging. De nucleaire of niet-nucleaire aard van de betrokken inrichtingen en installaties, is dus een van de parameters voor de indeling in categorieën.

Er wordt een onderscheid gemaakt tussen vijf categorieën van netwerk- en informatiesystemen, waarvan de eerste 2 categorieën systemen betreffen in de nucleaire sector, inclusief de nucleaire vervoerbedrijven, terwijl de andere systemen in sectoren voorkomen waar met radioactieve stoffen gewerkt wordt of waar deze aanwezig kunnen zijn. Dit kan zowel de medische als de industriële sector zijn.

Er wordt gekeken naar de netwerk- en informatiesystemen die zich bevinden in ofwel de "veiligheidszones" (in de zin van de nucleaire regelgeving) gedefinieerd voor kernmaterialen ofwel in de "beveiligde ruimte" (in de zin van het KB van 17 maart 2024 betreffende de beveiliging van radioactieve stoffen en bepaalde kernmaterialen) gedefinieerd voor radioactieve stoffen, alsook de netwerk- en informatiesystemen die op enigerlei wijze communiceren of verbonden zijn met deze zones of ruimtes. Door de koppeling tussen de netwerk- en informatiesystemen met de fysieke ruimtes of zones waar de kernmaterialen, de radioactieve stoffen of de nucleaire documenten en radiologische beveiligingsdocumenten aanwezig zijn, wordt er, weliswaar onrechtstreeks, rekening gehouden met de radiologische risico's volgens het principe van een graduele aanpak.

Wanneer radioactieve stoffen of kernmaterialen volledig of gedeeltelijk verwijderd worden uit de veiligheidszones of beveiligde ruimtes, waardoor de netwerk- en informatiesystemen van deze zones of ruimtes in een andere categorie worden ingedeeld, kunnen de netwerk- en informatiesystemen verbonden met de

d'information susmentionnés en fonction du caractère critique de ces réseaux et systèmes. La criticité à considérer prend également en compte les conséquences possibles de la compromission des systèmes et réseaux sur la sûreté et la sécurité nucléaires et radiologiques. La nature nucléaire ou non nucléaire des établissements et installations concernés, constitue ainsi un des paramètres de la répartition en catégories.

L'article distingue cinq catégories de réseaux et systèmes d'information, dont les deux premières catégories concernent des systèmes du secteur nucléaire, y inclus les entreprises de transport nucléaire, tandis que les autres réseaux et systèmes se retrouvent dans des secteurs où des substances radioactives sont utilisées ou peuvent être présentes ; il peut s'agir du secteur médical et du secteur industriel.

Sont ici visés les réseaux et systèmes d'information qui se trouvent soit dans des "zones de sécurité" (au sens de la réglementation nucléaire) définies pour les matières nucléaires, soit dans des "espaces sécurisés" (au sens de l'AR du 17 mars 2024 portant sur la sécurité des substances radioactives et de certaines matières nucléaires) définis pour des substances radioactives, ainsi que les réseaux et systèmes d'information qui communiquent avec ces zones ou espaces ou qui y sont reliés d'une quelconque manière. En liant les réseaux et systèmes d'information aux espaces ou zones physiques où se trouvent les matières nucléaires, les substances radioactives, les documents nucléaires ou les documents de sécurité radiologique, les risques radiologiques sont indirectement mais certainement pris en compte, et ce suivant le principe d'une approche graduée.

Lorsque des substances radioactives ou des matières nucléaires sont durablement retirées en tout ou en partie de zones de sécurité ou d'espaces sécurisés, et que cela entraîne la recatégorisation des réseaux et systèmes d'information de ces zones ou espaces, les réseaux et les systèmes d'information associés à ces zones ou

zones of ruimtes heringedeeld worden. Dit kan zich bijvoorbeeld voordoen bij de ontmanteling van installaties.

In **artikel 4** worden aan de netwerk- en informatiesystemen van in artikel 3 voorziene categorieën 1 tot en met 5, beveiligingsniveaus A tot en met D toegekend op basis van de gradatie van de cyberrisico's. Het hoogste beveiligingsniveau is A en het laagste is D. Binnen beveiligingsniveau A moeten de essentiële nucleaire cyberbeveiligingsmaatregelen worden genomen. Binnen beveiligingsniveau B de belangrijke nucleaire cyberbeveiligingsmaatregelen. Binnen beveiligingsniveau C de basis nucleaire cyberbeveiligingsmaatregelen. Binnen beveiligingsniveau D moeten ten slotte de nucleaire cyberbeveiligingsmaatregelen inzake behoedzaam beheer voorzien worden. Het is van belang te preciseren dat de principes van dit behoedzaam beheer zullen opgenomen worden in een technisch reglement van het Agentschap zoals voorzien is in artikel 17sexies, §2, van de wet van 15 april 1994 (zie artikel 5). In het verdere verloop van dit besluit zullen dan ook geen verdere verplichtingen opgelegd worden voor dit beveiligingsniveau. De specifieke essentiële, belangrijke en basis NCB-maatregelen worden verder in de tekst gespecificeerd.

Paragraaf 6 werd ingevoegd om duidelijkheid te scheppen over het toekennen van het beveiligingsniveau wanneer er binnen de inrichting netwerk- en informatiesystemen aanwezig zijn die ingedeeld kunnen worden in verschillende categorieën. In dat geval wordt het hoogste niveau toegekend aan alle systemen gezien de netwerksystemen over het algemeen steeds met elkaar verbonden zijn. In het uitzonderlijke geval dat een specifiek netwerk- en informatiesysteem toch voldoende onafhankelijk zou zijn en de exploitant dit kan aantonen, kan een lager beveiligingsniveau toegekend worden.

espaces peuvent également être recatégorisés. Cela peut se produire, par exemple, lors du démantèlement d'établissements.

L'article 4 attribue aux réseaux et systèmes d'information des catégories 1 à 5 visées à l'article 3 les niveaux de sécurité A à D, en fonction de la gradation des cyber-risques. Le niveau de sécurité A est le plus haut, le D est le plus bas. Les mesures de cybersécurité nucléaire essentielles doivent être prises au niveau de sécurité A, les mesures de cybersécurité nucléaire importantes au niveau de sécurité B, les mesures de cybersécurité nucléaire de base au niveau de sécurité C et, enfin, les mesures de cybersécurité nucléaire correspondant à une gestion prudente au niveau de sécurité D. Il est important de préciser que les principes de cette gestion prudente seront repris dans un règlement technique de l'Agence tel que le prévoit l'article 17sexies, §2, de la loi du 15 avril 1994 (voir article 5). Par conséquent, dans la suite du présent projet d'arrêté, aucune autre obligation ne sera imposée pour ce niveau de sécurité.

Les mesures de CSN essentielles, importantes et de base sont précisées plus loin dans le texte.

Le paragraphe 6 a été inséré pour clarifier l'attribution du niveau de sécurité dans le cas où l'établissement comporte des réseaux et systèmes d'information qui peuvent être classés dans des catégories différentes. Dans ce cas, le niveau le plus élevé est attribué à tous les systèmes dès lors que les réseaux et systèmes sont en général toujours interconnectés. Dans le cas exceptionnel où un réseau ou système d'information spécifique est suffisamment indépendant des autres, et pour autant que l'exploitant soit en mesure de le démontrer, le niveau de sécurité inférieur peut être retenu.

Artikel 5 bevat de bepalingen van het besluit die van toepassing zijn op het laagste beveiligingsniveau. Wanneer een exploitant de netwerk- en informatiesystemen van zijn inrichting heeft ingedeeld in categorie cyber -5, wordt een beveiligingsniveau D toegekend en zijn de principes van behoedzaam beheer van toepassing. De principes zijn niet verder uitgewerkt in dit besluit maar zullen het onderwerp uitmaken van een specifiek reglement van het Agentschap in toepassing van artikel 17sexies, §2 van de wet van 15 april 1994.

Artikel 6 bevat de algemene verplichtingen van een exploitant inzake nucleaire cyberbeveiliging, het nemen van passende maatregelen en het door de exploitant in te richten NCB-systeem. Dit artikel verplicht iedere exploitant van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in de eerste 4 categorieën om een NCB-systeem in te voeren, te onderhouden en continue te verbeteren.

Het NCB-systeem moet zodanig ontwikkeld worden dat hoe hoger het gevraagde beveiligingsniveau is hoe groter de garanties met betrekking tot de betrouwbaarheid en de efficiëntie moeten zijn. Dit wordt in de NIS-regelgeving de "maturiteit van het systeem" genoemd. Er moet steeds gestreefd worden naar het bereiken van het vereiste niveau door continue verbetering, ook in wijzigende omstandigheden.

Bij het inrichten van het NCB-systeem moet er rekening gehouden worden met het gevraagde beveiligingsniveau, met de bepalingen van dit ontwerpbesluit maar ook met een evaluatie van de cyberrisico's die beschouwd kunnen worden voor de netwerk- en informatiesystemen van de exploitant.

De exploitant dient bij het opstellen van het NCB-systeem ook rekening te houden met de "regels van goed vakmanschap". Het gaat hier bijvoorbeeld over aanbevelingen, standaarden, normen die van toepassing zijn in de cyberbeveiligingssector, alsook over aanbevelingen die het Internationaal Atoomenergieagentschap heeft

L'article 5 contient les dispositions de l'arrêté qui s'appliquent au niveau de sécurité le plus bas. Lorsqu'un exploitant a classé les réseaux et systèmes d'information de son établissement dans la catégorie cyber -5, un niveau de sécurité D est attribué et les principes de gestion prudente s'appliquent. Ces principes ne sont pas développés plus en détail dans le présent arrêté, mais feront l'objet d'un règlement spécifique de l'Agence en application de l'article 17sexies, §2, de la loi du 15 avril 1994.

L'article 6 concerne les obligations générales de l'exploitant en matière de cybersécurité nucléaire, la prise de mesures appropriées et l'établissement par l'exploitant du système de CSN.

Cet article oblige chaque exploitant d'un établissement dont les réseaux et systèmes d'information sont classés dans l'une des 4 premières catégories à établir, maintenir et améliorer en continu un système de CSN.

Le système de CSN doit être développé de telle sorte que plus le niveau de sécurité est élevé, plus les garanties concernant la fiabilité et l'efficacité doivent être importantes. Ceci est appelé la « maturité du système » dans la réglementation NIS. L'objectif est d'atteindre le niveau requis par une amélioration continue, même dans des circonstances changeantes.

Lors de la mise en place du système de CSN, il faut tenir compte du niveau de sécurité demandé, des dispositions du présent projet d'arrêté, mais également d'une évaluation des cyber-risques qui peuvent être considérés pour les réseaux et systèmes d'information de l'exploitant.

L'exploitant doit, lors de l'élaboration du système de CSN, également tenir compte des « règles de l'art ». Il s'agit ici de recommandations, de standards, de normes qui sont d'application dans le secteur de la cybersécurité ainsi que de recommandations que l'Agence internationale de l'énergie atomique édicte concernant la cybersécurité nucléaire.

uitgevaardigd met betrekking tot nucleaire cyberbeveiliging.

Deze "regels van goed vakmanschap" zijn onderworpen aan de snelle technische evolutie die eigen is aan deze sector.

Voor wat betreft de risicoanalyse moet vermeld worden dat deze een aanvulling is op de reeds gemaakte risicoanalyses met betrekking tot de fysieke beveiliging van de kernmaterialen en de radiologische beveiliging van radioactieve stoffen. Het is ook daarom dat er een verplichting voor de afgevaardigde voor NCB is om overleg te plegen met de afgevaardigde voor fysieke beveiliging en/of afgevaardigde voor radiologische beveiliging met betrekking tot de raakvlakken tussen de cyberrisico's en de risico's verbonden met de nucleaire beveiliging of radiologische beveiliging.

Bij het opstellen van het NCB-systeem moeten nucleaire cyberbeveiligingsmaatregelen (NCB-maatregelen) genomen worden die overeenkomen met de principes van een graduele aanpak: maatregelen die aangepast zijn aan het netwerk- en informatiesysteem zelf, het beveiligingsniveau dat werd toegekend en ook aan de geïdentificeerde risico's. Deze graduele aanpak is van toepassing op zowel de verschillende beveiligingsniveaus als op de te nemen NCB-maatregelen en op de mate waarin deze maatregelen worden toegepast.

Voor de technische vereisten van de verschillende nucleaire cyberbeveiligingsmaatregelen zal dit ontwerp besluit aangevuld worden met technische reglementen die zullen verwijzen naar het door het CCB opgesteld CyberFundamentals framework.

Het is ook aan de exploitant om te voorzien in het nemen van mogelijke bijkomende NCB-maatregelen wanneer hij kennis heeft van een specifieke dreiging tegen zijn inrichting, zijn installatie of zijn netwerk- en informatiesystemen of wanneer een dreiging vanuit een andere sector een mogelijke impact kan hebben op de inrichting van de exploitant.

Ces « règles de l'art » sont sujettes à l'évolution technique rapide qui est propre à ce secteur.

En ce qui concerne l'analyse de risque, il est à noter qu'il s'agit d'un complément aux analyses de risque concernant la protection physique des matières nucléaires et la sécurité radiologique des substances radioactives qui ont déjà été réalisées. C'est également pour cela que le délégué à la CSN doit obligatoirement consulter le délégué à la protection physique et/ou le délégué à la sécurité radiologique en ce qui concerne les interfaces entre les cyber-risques et les risques liés à la sécurité nucléaire ou la sécurité radiologique.

Lors de l'élaboration du système de CSN, des mesures de cybersécurité nucléaire (mesures de CSN) doivent être prises. Ces mesures doivent être conformes aux principes d'une approche graduée : des mesures qui sont adaptées aux réseaux et système d'information mêmes, au niveau de sécurité qui a été attribué et également aux risques qui ont été identifiés. Cette approche graduée s'applique aussi bien aux différents niveaux de sécurité, qu'aux mesures de CSN qui sont à prendre, qu'au degré d'application de ces mesures.

Ce projet d'arrêté sera complété par des règlements techniques qui feront référence au CyberFundamentals framework qui a été élaboré par le CCB en ce qui concerne les exigences techniques des différentes mesures de CSN.

Il appartient également à l'exploitant de prendre des mesures de cybersécurité nucléaire supplémentaires lorsqu'il a connaissance d'une menace spécifique contre son établissement, son installation ou son réseau et système d'information, ou quand une menace d'un autre secteur peut avoir un impact possible sur l'établissement de l'exploitant.

De derde paragraaf van artikel 6 vloeit voort uit de algemene cyberbeveiligingsplicht van de vorige paragrafen en schrijft voor dat de exploitant het NCB-systeem moet documenteren in een dossier, het "nucleair cyberbeveiligingsdossier"(NCB-dossier).

Het opstellen van het NCB-dossier is één van de elementen van de erkenningsprocedure van de nucleaire cyberbeveiligingsmaatregelen zoals vereist in artikel 17sexies, §1, 5°), van de Wet van 15 april 1994.

Bij de opmaak van het NCB-dossier moet de exploitant het advies inwinnen van de afgevaardigde voor NCB.

Artikel 7 bepaalt dat het NCB-systeem moet geïntegreerd zijn in de management-, kwaliteits- of beheersystemen van de exploitant. Er wordt geen specifieke normering hiervoor opgelegd.

Artikel 8 van dit ontwerp regelt de aanstelling van een afgevaardigde voor NCB. Dit kan volgens de eerste paragraaf van artikel 8, afhankelijk van de structuur of organisatie van de entiteit van de exploitant, iemand binnen de organisatie zijn of iemand extern, zolang er bij deze laatste een duurzame relatie is met de exploitant. Er is geen verplichting opgenomen om ook een back-up afgevaardigde aan te stellen maar in grotere ondernemingen is dit wel een goede praktijk.

De exploitant moet mogelijke belangenconflicten vermijden in hoofde van de afgevaardigde voor NCB. Die moet naar het voorbeeld van o.a. de functionaris voor de gegevensbescherming (Data Protection Officer of DPO) een onafhankelijke en onpartijdige persoon zijn binnen de organisatie. Combinatie met functies in het hogere management worden best vermeden.

Deze afgevaardigde moet beschikken over de nodige opleidingen of ervaring betreffende cyberbeveiliging. Hij moet deze vorming of ervaring kunnen aantonen.

De geschikte vorming kan aangetoond worden door bijvoorbeeld de volgende

Le troisième paragraphe de l'article 6 découle de l'obligation générale de cybersécurité visée aux paragraphes précédents et dispose que l'exploitant doit documenter le système de CSN dans un dossier, le « dossier de cybersécurité nucléaire » (dossier de CSN).

L'établissement du dossier de CSN constitue l'un des éléments de la procédure d'agrément des mesures de cybersécurité nucléaire, requise par l'article 17sexies, §1,5°), de la Loi du 15 avril 1994.

Pour élaborer son dossier de CSN l'exploitant doit solliciter l'avis du délégué à la CSN.

L'article 7 dispose que le système de CSN doit être intégré aux systèmes de management, de qualité ou de gestion de l'exploitant. Aucune norme spécifique n'est imposée.

L'article 8 du présent projet régit la désignation d'un délégué à la CSN. En vertu du premier paragraphe de l'article 8, il peut s'agir, selon la structure ou l'organisation de l'entité de l'exploitant, soit d'une personne interne à l'organisation, soit d'une personne externe, pour autant que celle-ci entretienne une relation durable avec l'exploitant. Il n'est pas obligatoire de désigner un délégué suppléant, bien qu'il s'agisse d'une bonne pratique dans les entreprises de plus grande taille.

L'exploitant veille à éviter tout conflit d'intérêts potentiel dans le chef du délégué à la CSN. Sur le modèle du délégué à la protection des données (Data Protection Officer ou DPO), il doit s'agir d'une personne indépendante et impartiale au sein de l'organisation. Le cumul avec des fonctions de haut management doit être évité.

Ce délégué doit posséder la formation ou l'expérience nécessaire en matière de cybersécurité. Il doit être capable de démontrer cette formation ou cette expérience.

La formation appropriée peut, par exemple, être justifiée par les certificats, attestations,

certificatie, getuigschriften, beroepsopleidingen, diploma's:

- Certified Information Systems Auditor (CISA),
- Certified Information Security Manager (CISM),
- Certified Information Systems Security Professional (CISSP)
- Een bachelor of master in informatieveiligheid of cyberbeveiliging, dan wel een evenwaardig diploma.

Kennis van het wetgevend kader met betrekking tot cyberbeveiliging in het algemeen en NCB in het bijzonder is eveneens aangewezen voor deze functie.

In deze snel veranderende sector is het van primordiaal belang dat deze afgevaardigde zijn kennis permanent up-to-date houdt.

De aanstelling moet overeenkomstig de derde paragraaf van artikel 8 goedgekeurd worden door het Agentschap.

Indien de aangestelde afgevaardigde voor NCB de functie niet meer uitoefent, dient dit onmiddellijk aan het Agentschap gemeld te worden. De verantwoordelijkheden kunnen dan overgenomen worden door een back-up afgevaardigde die reeds eerder werd goedgekeurd door het Agentschap of die nog moet goedgekeurd worden..

Artikel 9 van dit ontwerp van koninklijk besluit regelt de opdrachten van de afgevaardigde voor NCB. Het is belangrijk aan te geven dat de eindverantwoordelijkheid van de NCB bij de exploitant berust, zoals voorzien in §15 van dit artikel. Het is evident dat het ook aan de exploitant is om indien nodig op te treden wanneer de regels niet gevolgd worden. Het is de opdracht en de taak van de afgevaardigde voor NCB om de exploitant hierin bij te staan en het nucleair cyberbeveiligingssysteem uit te voeren en daarvoor de nodige NCB-maatregelen op te zetten. Dit gebeurt onder de verantwoordelijkheid van de exploitant. De exploitant dient er dan ook voor te zorgen dat de afgevaardigde voldoende en tijdig betrokken wordt bij elke aangelegenheid die te maken heeft met de NCB.

formations professionnelles ou diplômes suivants :

- Certified Information Systems Auditor (CISA),
- Certified Information Security Manager (CISM),
- Certified Information Systems Security Professional (CISSP),
- un baccalauréat ou un master en sécurité de l'information ou en cybersécurité, ou un diplôme équivalent.

La connaissance du cadre législatif relatif à la cybersécurité en général et à la CSN en particulier est également conseillée pour cette fonction.

Dans ce secteur en évolution rapide, il est primordial que ce délégué maintienne ses connaissances à jour en permanence.

La désignation doit être approuvée par l'Agence, conformément au troisième paragraphe de l'article 8.

Si le délégué à la CSN qui a été désigné n'exerce plus cette fonction, il doit en avvertir l'Agence sans délai. Ses responsabilités peuvent alors être reprises par un délégué suppléant qui a déjà été approuvé par l'Agence précédemment ou qui doit encore l'être.

L'article 9 du présent projet d'arrêté royal régit les missions du délégué à la CSN. Il est important de souligner que la responsabilité finale de la CSN incombe à l'exploitant, comme prévu au §15 du présent article. Il va de soi qu'il appartient également à l'exploitant d'intervenir si nécessaire lorsque les règles ne sont pas respectées. Il relève de la mission et des tâches du délégué à la CSN d'assister l'exploitant et de mettre en œuvre le système de CSN et d'adopter les mesures de CSN nécessaires, bien qu'il exerce cette mission et ces tâches sous la responsabilité de l'exploitant. Celui-ci doit dès lors faire en sorte que le délégué à la CSN soit impliqué suffisamment et en temps utile dans toutes les questions qui touchent à la CSN.

De afgevaardigde voor NCB moet ook voldoende gekend zijn bij iedereen binnen de entiteit van de exploitant.

Tevens moeten hem, overeenkomstig paragraaf 2 van artikel 9, de nodige ondersteuning, tijd en middelen ter beschikking worden gesteld voor de uitoefening van zijn taken alsook, voor het in stand houden van zijn deskundigheid. Gezien de snelle technologische evoluties en de steeds wijzigende cyber-risico's is dit van primordiaal belang.

Paragraaf 4 van artikel 9 omschrijft één van de meest essentiële taken van de afgevaardigde voor NCB, namelijk het informeren en adviseren van de exploitant en zijn medewerkers over alles wat met NCB te maken heeft, zowel juridisch als technisch. De afgevaardigde voor NCB moet onmiddellijk geraadpleegd worden in geval van een cyberincident. Ook is zijn advies of bijstand vereist bij elke belangrijke beslissing die gevolgen kan hebben voor de NCB van de exploitant (paragraaf 5).

De zesde paragraaf van artikel 9 omschrijft een andere essentiële taak van de afgevaardigde voor NCB, namelijk het toezien op de naleving van het NCB-systeem van de exploitant dat door of op advies van de afgevaardigde voor NCB werd uitgewerkt. Naar het voorbeeld van de functionaris voor de gegevensbescherming (DPO) moet de afgevaardigde voor NCB het eerste contactpunt zijn inzake NCB, zowel intern voor de medewerkers van de exploitant als extern ten aanzien van derden of bevoegde autoriteiten en dit zonder afbreuk te doen aan de verantwoordelijkheden van de exploitant.

De achtste paragraaf van artikel 9 kadert in de interne bewustwording onder de medewerkers van de exploitant waarbij de afgevaardigde voor NCB een centrale rol speelt. Hij moet in het bijzonder zorgen voor de nodige bewustwording door het geven van opleidingen en het verstrekken van informatie aan de medewerkers.

Paragraaf 10 van artikel 9 sluit aan op de essentiële toezichthoudende taak van de afgevaardigde voor NCB met betrekking tot het door de exploitant ingestelde NCB-systeem. Het niet toepassen van het

Le délégué à la CSN doit également être suffisamment connu de tous au sein de l'entité de l'exploitant.

Il doit en outre bénéficier de l'assistance, du temps et des ressources nécessaires à l'exercice de ses tâches, en vertu du paragraphe 2 de l'article 9 ainsi que pour entretenir son expertise. C'est même primordial si l'on considère la rapidité des évolutions technologiques et la constante mutation des cyber-risques.

Le paragraphe 4 de l'article 9 décrit une des tâches essentielles du délégué à la CSN, qui consiste à informer et à conseiller l'exploitant et ses collaborateurs sur tout ce qui a trait à la CSN, tant sur le plan juridique que technique. Le délégué à la CSN doit être consulté immédiatement en cas de cyber-incident. Son avis ou son aide sont également requis lors de toute décision importante susceptible d'affecter la CSN de l'exploitant (paragraphe 5).

Le sixième paragraphe de l'article 9 décrit une autre tâche essentielle du délégué à la CSN, qui consiste à contrôler le respect du système de CSN de l'exploitant qui a été établi par ses soins ou sur ses conseils. À l'instar du délégué à la protection des données (DPO), le délégué à la CSN doit être le point de contact privilégié en matière de CSN, tant en interne pour le personnel de l'exploitant qu'en externe pour les tiers ou les autorités compétentes, sans préjudice des responsabilités de l'exploitant.

Le huitième paragraphe de l'article 9 s'inscrit dans le cadre de la conscientisation en interne du personnel de l'exploitant, le délégué à la CSN étant appelé à y jouer un rôle central. Il est en particulier chargé de veiller à la conscientisation nécessaire en organisant des formations et des séances d'informations destinées au personnel.

Le paragraphe 10 de l'article 9 se rapporte à la tâche essentielle de contrôle du délégué à la CSN par rapport au système de CSN mis en place par l'exploitant. Le non-respect du système doit être immédiatement

systeem moet door de afgevaardigde voor NCB onmiddellijk gemeld worden aan de exploitant.

Paragraaf 11 van artikel 9 voorziet in de verplichting voor de afgevaardigde voor NCB een jaarverslag op te maken dat ter inzage van het Agentschap moet worden gehouden en in een aantal minimumvereisten wat de inhoud van dit jaarverslag betreft.

Niet onbelangrijk is paragraaf 13 waarin expliciet opgenomen is dat de afgevaardigde zich kan laten bijstaan door of advies kan inwinnen bij externe partijen. In een snel veranderende hoogtechnologische omgeving is het vaak noodzakelijk om bijkomende expertise te raadplegen.

Paragraaf 14 stelt dat er overleg nodig is tussen de verantwoordelijken voor beveiliging, zowel fysieke beveiliging als cyberbeveiliging, maar legt ook een verplichting op om te overleggen met de dienst voor fysieke controle om zo de raakvlakken tussen beveiliging en nucleaire, radiologische veiligheid en stralingsbescherming te kunnen beheren.

Artikel 10 bepaalt dat de exploitant instaat voor de nodige vorming van zijn personeel en in het bijzonder die van de afgevaardigde voor NCB. Deze afgevaardigde is, zoals eerder bepaald, een belangrijke schakel in het opzetten en onderhouden van het NCB-systeem en de daarbij horende NCB-maatregelen.

Naast de informatie en sensibilisering van eigen personeel is het ook van belang dat er aandacht besteed wordt aan de externe partijen die toegang kunnen hebben tot de netwerk- en informatiesystemen.

Artikel 11 verwijst naar de andere relevante regelgevingen met betrekking tot nucleaire en radiologische beveiligingsdocumenten. Deze regelgevingen zijn voornamelijk vermeld in het Koninklijk besluit van 17 oktober 2011 houdende de categorisering en de bescherming van nucleaire documenten, het koninklijke besluit van 17 maart 2024

communiqué par le délégué à la CSN à l'exploitant.

Le paragraphe 11 de l'article 9 prévoit l'obligation pour le délégué à la CSN d'établir un rapport annuel qui doit être tenu à la disposition de l'Agence à des fins de consultation, et énumère certaines exigences minimales concernant le contenu de ce rapport annuel.

Le paragraphe 13 n'est pas sans importance dans la mesure où il prévoit explicitement la possibilité pour le délégué de se faire assister par des parties extérieures ou de leur demander conseil. Dans un environnement hautement technologique en rapide mutation, il est souvent nécessaire de pouvoir compter sur une expertise complémentaire.

Le paragraphe 14 dispose qu'une consultation entre les responsables de la sécurité, aussi bien la sécurité physique que la cybersécurité, est nécessaire, mais impose également l'obligation de consulter le service de contrôle physique afin de pouvoir gérer les interfaces entre la sécurité, la sûreté nucléaire et radiologique et la radioprotection.

L'article 10 détermine que l'exploitant est responsable de prévoir la formation nécessaire de son personnel et, en particulier, du délégué à la CSN. Ce délégué est, comme stipulé plus loin, un maillon important dans l'établissement et le maintien du système de CSN et des mesures de CSN qui en découlent.

Outre l'information et la sensibilisation du personnel interne, il est également important de prêter attention aux parties externes qui peuvent avoir accès aux réseaux et aux systèmes d'information.

L'article 11 renvoie aux autres réglementations pertinentes en matière de documents relatifs à la sécurité nucléaire et radiologique. Elles figurent principalement dans l'arrêté royal du 17 octobre 2011 portant sur la catégorisation et à la protection des documents nucléaires, l'arrêté royal du 17 mars 2024 relatif à la sécurité des substances radioactives et de

betreffende de beveiliging radioactieve stoffen en bepaalde kernmaterialen en het Koninklijk besluit van 17 maart 2024 betreffende de beveiliging van inrichtingen voor bovengrondse berging van radioactief afval. Deze regelgevingen bevatten specifieke bepalingen ter bescherming van documenten en informatie die moet gegarandeerd blijven.

Hoofdstuk IV omvat de NCB-maatregelen. Deze zijn opgebouwd rond vijf functies die het NCB-systeem moet garanderen: identificeren, beschermen, detecteren, reageren en herstellen, zoals voorzien in het CyberFundamentals framework opgesteld door het CCB.

De identificatiemaatregelen bevatten onder meer de verplichting voor de exploitant om de elementen van zijn netwerk- en informatiesystemen en de middelen te inventariseren, de rollen en verantwoordelijkheden binnen zijn organisatie vast te leggen, risico's te identificeren en te beheren en kwetsbaarheden te identificeren. Ook de gegevens- en informatiestromen moeten in kaart gebracht worden, gedocumenteerd en continu bijgewerkt worden. Het documenteren van deze gegevensstromen houdt ook in dat deze stromen door de exploitant moeten goedgekeurd worden en dat deze goedkeuring op een of andere wijze bewaard wordt. De inventarisatie van de middelen moet ruim gezien worden en bevat o.a. ook hardware, apparaten, gegevens, informatie, software, ...

Wanneer het gaat over het bepalen van de cyberrisico's in de toeleveringsketen, is het aan de exploitant om passende maatregelen op te nemen in de overeenkomsten die met leveranciers worden gesloten. Deze maatregelen dienen in overeenstemming te zijn met het nucleair cyberbeveiligingsbeleid van de exploitant. Het naleven van de contractuele verplichtingen dient beoordeeld te worden aan de hand van audits, testresultaten en andere evaluaties.

De beschermingsmaatregelen bevatten onder meer de verplichting om de toegang

certaines matières nucléaires et l'arrêté royal du 17 mars 2024 relatif à la sécurité des installations de stockage en surface de déchets radioactifs. Ces réglementations contiennent des dispositions spécifiques visant à garantir la protection des documents et des informations.

Le **chapitre IV** contient les mesures de CSN. Celles-ci s'articulent autour des cinq fonctions qui doivent être garanties par le système de CSN : identifier, protéger, détecter, répondre et rétablir, tel que prévu par le CyberFundamentals framework élaboré par le CCB.

Les **mesures d'identification** concernent notamment l'obligation pour l'exploitant d'inventorier les éléments de ses réseaux et systèmes d'information et ses ressources, de définir les rôles et les responsabilités au sein de son organisation, d'identifier et de maîtriser les risques et d'identifier les vulnérabilités. De même, les flux de données et d'informations doivent être schématisés, documentés et mis à jour de manière continue. La documentation de ces flux de données signifie également que ces flux doivent être approuvés par l'exploitant et que cette approbation doit être conservée d'une manière ou d'une autre. L'inventaire des ressources doit être compris au sens large et il inclut notamment le hardware, les appareils, les données, les informations, les logiciels, etc.

En ce qui concerne l'identification des cyber-risques dans la chaîne d'approvisionnement, il appartient à l'exploitant de prévoir des mesures appropriées dans les accords conclus avec les fournisseurs. Ces mesures doivent être conformes à la politique de cybersécurité nucléaire de l'exploitant. Le respect des obligations contractuelles doit être apprécié sur la base d'audits, de résultats de tests et d'autres évaluations.

Les **mesures de protection** concernent notamment l'obligation de gérer l'accès aux

tot systemen te beheren, authenticatieniveaus te bepalen, netwerken en applicaties af te schermen, opleidingen inzake NCB te voorzien, technische beveiligingsmaatregelen te nemen zoals encryptie, logging, e.d.

Er wordt verplicht om kritieke en gevoelige gegevens te beschermen. Dit kunnen gegevens van allerlei aard zijn. Het betreft o.a. gegevens die de bedrijfszekerheid of de nucleaire beveiliging, veiligheid en stralingsbescherming in het gedrang kunnen brengen. Gevoelige gegevens kunnen vb. deze gegevens zijn die omwille van andere regelgevingen moeten beschermd worden of die zich in de privésfeer bevinden.

Ook activa en media moeten beschermd worden. Activa (bedrijfsmiddelen/assets) verwijzen naar mensen, apparatuur, software, gegevens of andere elementen van informatiesystemen van een organisatie die waarde hebben en beschermd moeten worden. Extra maatregelen moeten er genomen worden voor gebruikers met verhoogde toegangsrechten, dit wil zeggen gebruikers met een hogere machtiging binnen de systemen. Deze gebruikers, zoals systeembeheerders, kunnen de infrastructuur beheren, en daardoor toegang krijgen tot gevoelige systemen en data.

De detectiemaatregelen met verplichtingen inzake het vaststellen, documenteren, beheren, analyseren en evalueren van cyberincidenten. Het vaststellen van cyberincidenten heeft zowel betrekking op het vaststellen van aanvallen van buiten uit als op het onderzoeken of bepaalde geïdentificeerde risico's ook in de eigen systemen aanwezig zijn (insider threat).

Het monitoren van de activiteiten van het eigen personeel, maar ook van die van externen binnen het netwerk- en informatiesysteem heeft als doel abnormaliteiten te detecteren die mogelijk schade kunnen berokkenen. Uiteraard dient dit te gebeuren in volledige overeenstemming met de regelgeving met betrekking tot de wet van 30 juli 2018 betreffende de bescherming van natuurlijke

systèmes, de déterminer les niveaux d'authentification, de protéger les réseaux et les applications, d'organiser des formations en CSN, d'adopter des mesures de sécurité techniques, telles que le cryptage, le logging, etc.

Il est obligatoire de protéger les données sensibles et critiques. Ces données peuvent être de tout ordre. Elles peuvent être de nature à compromettre la sécurité opérationnelle ou la sécurité nucléaire, la sûreté et la radioprotection, etc. Les données sensibles peuvent, par exemple, être des données qui doivent être protégées en vertu d'autres réglementations ou qui relèvent de la sphère privée.

Les actifs et les supports doivent également être protégés. Les actifs (assets) désignent des personnes, des dispositifs, des softwares, des données ou autres éléments des systèmes d'information d'une organisation qui ont une valeur et doivent être protégés. Des mesures supplémentaires doivent être prises pour les utilisateurs disposant de droits d'accès étendus, c'est-à-dire les utilisateurs ayant une autorisation plus élevée au sein des systèmes. Ces utilisateurs, tels que les administrateurs système, peuvent gérer l'infrastructure et par conséquent avoir accès à des systèmes et à des données sensibles.

Les **mesures de détection** impliquent l'obligation de constater, documenter, gérer, analyser et évaluer les cyber-incidents. La constatation des cyber-incidents couvre aussi bien la constatation d'attaques extérieures que l'étude pour déterminer si certains risques identifiés sont également présents dans les systèmes de l'exploitant (insider threat).

La surveillance des activités du personnel de l'exploitant mais également de personnes extérieures au sein des réseaux et systèmes d'information a pour finalité de détecter toute anomalie de nature à porter préjudice. Bien entendu, cela doit se faire dans le plein respect de la réglementation liée à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

personen met betrekking tot de verwerking van persoonsgegevens.

Respons- en herstelmaatregelen omvatten verplichtingen en te nemen maatregelen om tijdig te reageren op cyberincidenten, die te melden, te analyseren, de gevolgen ervan te beperken en te herstellen. Een belangrijk element is het trekken van lessen uit elk incident om zo de beveiliging van de netwerk- en informatiesystemen te verbeteren.

In de **artikelen 12 en, 13 en 14** zijn de essentiële, de belangrijke en de basis nucleaire cyberbeveiligingsmaatregelen opgenomen.

De Basis NCB-maatregelen bieden een betrouwbaar beschermingsniveau door gebruik te maken van technologieën en processen die over het algemeen beschikbaar zijn. Waar nodig kunnen deze NCB maatregelen worden aangepast en verbeterd om beter aan te sluiten bij de specifieke behoeften van de inrichting.

De Belangrijke NCB-maatregelen versterken de basis NCB-maatregelen om de impact van bekende cyberrisico's te verminderen en om de impact van aanvallen door actoren met courante middelen en vaardigheden te beperken.

Met de essentiële NCB-maatregelen worden de belangrijke NCB-maatregelen verder versterkt om te voldoen aan de hoogste cyberbeveiligingsvereisten.

Deze maatregelen omvatten geavanceerde beveiligingsfuncties en zijn ontworpen om stand te houden tegen geavanceerde cyberaanvallen uitgevoerd door actoren met aanzienlijke middelen en expertise.

In elk van de artikelen 12, 13 en 14 is opgenomen dat het Agentschap technische reglementen kan opstellen waarin deze maatregelen verder gedetailleerd zullen worden. Deze technische reglementen zullen verwijzen naar het CyberFundamentals framework opgesteld door het CCB. Er kan eveneens rekening worden gehouden met de relevante inzichten opgenomen in andere normen of kaders inzake informatieveiligheid

Les **mesures de réponse et de rétablissement** couvrent les obligations et les mesures à prendre pour répondre aux cyber-incidents, les notifier, les analyser, en limiter les conséquences et procéder au rétablissement de la situation en temps utile. Un des éléments importants ici est de tirer les enseignements utiles de chaque incident pour améliorer de la sorte la sécurité des réseaux et systèmes d'information.

Les articles 12, 13 et 14 prévoient les mesures de cybersécurité nucléaire essentielles, importantes et de base.

Les mesures de CSN de base offrent un niveau de protection fiable grâce à l'utilisation de technologies et de processus généralement disponibles. Si nécessaire, ces mesures de CSN peuvent être adaptées et améliorées afin de mieux répondre aux besoins spécifiques de l'établissement.

Les mesures de CSN importantes renforcent les mesures de CSN de base afin de réduire l'impact des cyber-risques connus et de limiter l'impact des attaques menées par des acteurs disposant de moyens et de compétences limités.

Les mesures de CSN essentielles renforcent encore les mesures de CSN importantes afin de répondre aux exigences les plus élevées en matière de cybersécurité. Ces mesures comprennent des fonctions de sécurité avancées et sont conçues pour résister à des cyberattaques sophistiquées menées par des acteurs disposant de moyens et d'une expertise considérables.

Dans chacun des articles 12, 13 et 14, il est prévu que l'Agence peut élaborer des règlements techniques dans lesquelles ces mesures seront détaillées. Ces règlements techniques feront référence au CyberFundamentals framework préparé par le CCB. Ils pourront prendre également en compte les éléments pertinents inclus dans d'autres normes ou cadres sur la sécurité de l'information et/ou la cybersécurité tels que,

en/of cyberbeveiliging, zoals bijvoorbeeld NIST/CFS, ISO 27001/ISO 27002, IEC 62443 en de CIS Controls (ETSI TR 103 305-1) of de Nuclear Security Series (NSS-17-T, NSS-42-G) van het IAEA.

Artikel 15 legt verplichtingen op om het NCB-systeem periodiek te testen. Deze testen dienen met een zekere regelmaat te gebeuren rekening houdend met de meest recente incidenten en dreigingen. Bij de voorbereiding van deze testen kan de exploitant vb. gebruik maken van de resultaten van eventuele tussentijdse simulaties en andere oefeningen. De resultaten van deze testen moeten geëvalueerd worden en, indien nodig, moeten bijkomende maatregelen genomen worden. Het is niet de bedoeling het resultaat van deze testen systematisch aan het Agentschap over te maken maar enkel ter beschikking te houden indien het Agentschap daarnaar vraagt.

Artikel 16 vraagt geen verdere toelichting

Artikel 17, eerste paragraaf, van dit ontwerpbesluit regelt de adequate uitwisseling tussen de in artikel 16 vermelde autoriteiten (het Agentschap en het CCB) van informatie over cyberrisico's of cyberincidenten waarmee exploitanten kunnen worden geconfronteerd. De doelstelling hiervan is om het mogelijk te maken dat deze autoriteiten op het gebied van cyberbeveiliging hun medewerking, advies en ervaring ter beschikking kunnen stellen van de nucleaire cyberbeveiliging.

In de tweede paragraaf van artikel 17 wordt verduidelijkt dat er tevens moet rekening gehouden worden met de vereisten van vertrouwelijkheid, beroepsgeheim of andere beperkingen in toepasselijke wetgeving, onder meer de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn

par exemple, NIST/CFS, ISO 27001/ISO 27002, IEC 62443 et les CIS Controls (ETSI TR 103 305-1), ou les Nuclear Security Series (NSS-17-T, NSS-42-G) de l'IAEA.

L'article 15 concerne les obligations de tester périodiquement le système de CSN. Ces tests doivent être réalisés avec une certaine régularité de sorte qu'ils puissent tenir compte des incidents et des menaces les plus récents. Lors de la préparation de ces tests, l'exploitant peut notamment utiliser les résultats d'éventuels exercices intermédiaires de simulations ou d'autres tests. Les résultats de ces tests doivent être évalués et, si nécessaire, des mesures supplémentaires doivent être adoptées. L'intention n'est pas que les résultats de ces tests soient systématiquement transmis à l'Agence, mais que l'Agence ait la possibilité de les consulter si elle en fait la demande.

L'article 16 ne demande pas de commentaire particulier.

L'article 17, premier paragraphe, du présent projet d'arrêté régit l'échange entre les autorités mentionnées à l'article 16 (l'Agence et le CCB) des informations sur les cyber-risques ou cyber-incidents auxquels peuvent être confrontés les exploitants. L'objectif est que ces autorités compétentes dans les domaines de la cybersécurité puissent mettre leur collaboration, leurs conseils et leur expérience au service de la cybersécurité nucléaire.

Le deuxième paragraphe de l'article 17 précise que l'on prend également en compte les exigences en matière de confidentialité et de secret professionnel ou d'autres restrictions contenues dans la législation applicable, notamment dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

95/46/EG (algemene verordening gegevensbescherming).

(règlement général sur la protection des données).

Hoofdstuk VI bevat de bepalingen voor wat betreft de erkenningsprocedure van de NCB-maatregelen die samenvattend kunnen beschreven zijn in het NCB-dossier.

Gezien de snelle technologische evolutie van de sector en de maatregelen die genomen kunnen of moeten worden, is ervoor gekozen om te zorgen voor stabiliteit in de erkenning en het vermijden van een veelvuldig wijzigingsproces van deze erkenning.

Dit hoofdstuk behandelt de inhoud van het NCB-dossier en het proces voor nieuwe exploitanten en houdt ook rekening met de graduele aanpak.

Voor exploitanten die reeds actief zijn, zijn er verder in dit ontwerp overgangsmaatregelen gedefinieerd. Dit zijn exploitanten die reeds vergund zijn volgens de bepalingen van het algemeen reglement, de bestaande nucleaire installaties of nucleaire vervoerbedrijven die een erkend fysiek beveiligingssysteem hebben.

De eerste paragraaf van **artikel 18** bepaalt dat de exploitanten die een NCB-dossier moeten opstellen, diegene zijn die ook nucleaire of radiologische beveiligingsmaatregelen voor wat betreft de radioactieve stoffen of kernmaterialen moeten nemen, volgens de bepalingen van het KB van 17 maart 2024 betreffende de beveiliging van radioactieve stoffen en bepaalde kernmaterialen (hierna KB-RAMAS) of de KB's van 17 oktober 2011, die de belangrijkste delen zijn van de regelgeving met betrekking tot nucleaire en radiologische beveiliging.

De tweede paragraaf van dit artikel heeft betrekking op het geval dat er in eenzelfde inrichting meerdere onafhankelijke netwerken informatiesystemen aanwezig zijn waar een verschillend beveiligingsniveau aan werd toegekend. In dit geval zal de exploitant elk van zijn onafhankelijke systemen in het een NCB-dossier moeten opnemen.

Wanneer een bestaande exploitant een nieuwe installatie wil integreren in zijn

Le **chapitre VI** contient les dispositions relatives à la procédure d'agrément des mesures de CSN qui peuvent être sommairement décrites dans le dossier de CSN.

Compte tenu de l'évolution rapide de la technologie dans le secteur et des mesures qui peuvent ou doivent être prises, il a été choisi de garantir une stabilité au niveau de l'agrément et d'éviter une multitude de modifications de cet agrément.

Ce chapitre traite du contenu du dossier de CSN et de la procédure pour les nouveaux exploitants, et intègre l'approche graduée.

Pour les exploitants déjà en activité, des mesures transitoires sont définies plus loin dans le présent projet. Ce sont des exploitants déjà autorisés en vertu des dispositions du règlement général, des installations nucléaires existantes ou des entreprises de transport nucléaire qui ont un système de protection physique agréé.

Le premier paragraphe de l'**article 18** détermine que les exploitants qui doivent établir un dossier de CSN sont ceux qui doivent également prendre des mesures de sécurité nucléaire ou radiologique à l'égard de substances radioactives ou de matières nucléaires, conformément aux dispositions de l'AR du 17 mars 2024 portant sur la sécurité des substances radioactives et de certaines matières nucléaires (ci-après AR RAMAS) ou des AR du 17 octobre 2011, qui constituent les principaux volets de la réglementation de la sécurité nucléaire et radiologique.

Le second paragraphe de cet article porte sur le cas où il y aurait plusieurs réseaux et systèmes d'information indépendants dans le même établissement ayant reçu un niveau différent de sécurité. Dans ce cas, l'exploitant devra reprendre chacun de ses systèmes indépendants dans le dossier de CSN.

Si un exploitant existant souhaite intégrer une nouvelle installation dans son

inrichting, zal het NCB-systeem van deze nieuwe installatie moeten voldoen aan het vereiste niveau van de reeds aanwezige netwerk- en informatiesystemen, tenzij dit volledig onafhankelijk zou zijn.

In de derde paragraaf van artikel 18 wordt de minimale inhoud van het NCB-dossier opgesomd voor een nieuwe inrichting. De exploitant van een volledig nieuwe inrichting moet het ontwerp van zijn NCB-systeem aan een zelfevaluatie onderwerpen waarbij wordt nagegaan of het vereiste niveau zal bereikt worden. Voor het uitvoeren van deze zelfevaluatie kan er gebruik gemaakt worden van de hulpmiddelen die hiervoor ontwikkeld werden door het CCB en ter beschikking zijn op hun website.

Artikel 19 vraagt geen verdere toelichting.

Artikel 20 vraagt geen verdere toelichting.

De in **artikel 21** opgenomen externe audit dient te gebeuren door een conformiteitsbeoordelingsinstantie die geaccrediteerd is door een nationale accreditatie-instantie en erkend werd door het CCB of door een andere externe organisatie gespecialiseerd in cyberbeveiliging, in ieder geval door een van de exploitant onafhankelijke organisatie.

Artikel 22 behandelt de wijzigingen aan de netwerk- en informatiesystemen. Gezien het gaat over een snel wijzigende technische sector is het praktisch niet mogelijk om een meldingsplicht in te voeren voor elke wijziging. De meldingsplicht geldt dan ook enkel voor die wijzigingen waardoor de netwerk- en informatiesystemen in een andere categorie moeten worden ingedeeld.

Artikel 23 bepaalt dat de exploitant de beveiliging van zijn netwerk- en informatiesystemen op periodieke basis moet auditeren en laten auditeren. Rekening houdend met een graduele aanpak zijn de frequenties van de audits verschillend voor

établisement, le système de CSN de cette nouvelle installation devra atteindre le niveau requis des réseaux et systèmes d'information déjà existants, à moins qu'il ne soit complètement indépendant.

Le troisième paragraphe de l'article 18 précise le contenu minimum du dossier de CSN pour un nouvel établissement. L'exploitant d'une nouvelle installation doit procéder à une auto-évaluation de son projet de système de CSN, en vérifiant si le niveau requis sera atteint. Pour réaliser cette auto-évaluation, il peut utiliser les outils développés par le CCB et disponibles sur son site web.

L'article 19 ne demande pas de commentaire particulier.

L'article 20 ne demande pas de commentaire particulier.

L'audit externe prévu à **l'article 21** doit être réalisé par un organisme d'évaluation de la conformité accrédité par un organisme national d'accréditation et reconnu par le CCB ou par une autre organisation externe spécialisée dans la cybersécurité, en tout état de cause par une organisation indépendante de l'opérateur.

L'article 22 traite des modifications apportées aux réseaux et systèmes d'information. Au égard à l'évolution rapide de ce secteur technique, il n'est pas possible dans les faits de rendre obligatoire la notification de chaque modification. L'obligation de notification ne s'applique donc qu'aux seules modifications qui entraînent un changement de catégorie dans laquelle sont classés les réseaux et systèmes d'information.

L'article 23 contient l'obligation pour l'exploitant de soumettre la sécurité de ses réseaux et systèmes d'information à des audits périodiques. Compte tenu de l'approche graduée, la fréquence des audits varie selon les catégories. Les audits

de verschillende categorieën. De externe audits moeten uitgevoerd worden door instanties die daarvoor geaccrediteerd zijn. Deze accreditatie dient te gebeuren door een nationale accreditatie-instantie. Deze moet geldig zijn voor het beveiligingsniveau dat aan de audit wordt onderworpen. Deze autoriteit is voorzien in de NIS2-wet. Na de accreditatie moet de auditororganisatie ook erkend worden door het CCB.

Artikel 24 vraagt geen verdere toelichting.

Hoofdstuk IX behandelt de overgangsbepalingen voor exploitanten die onder de toepassing van dit ontwerpbesluit vallen en die op het ogenblik van de inwerkingtreding van dit besluit reeds door het Agentschap vergund of erkend zijn. Deze overgangsmaatregelen zijn eveneens van toepassing op exploitanten van een nucleaire installatie of een nucleair vervoerbedrijf die reeds in het bezit zijn van een erkend fysiek beveiligingssysteem of een erkend algemeen beveiligingssysteem. Voor deze exploitanten wordt een overgangsperiode voorzien zodat zij de tijd krijgen zich in regel te stellen met dit ontwerpbesluit. Het NCB-dossier moet ook voor deze exploitanten een zelfevaluatie bevatten. Deze zelfevaluatie, die eveneens met de hulpmiddelen van het CCB kan uitgevoerd worden, moet een stand van zaken geven van het niveau van het bestaande NCB-systeem ten overstaan van het vereiste niveau. Het resultaat van deze zelfevaluatie moet gebruikt worden om een actieplan op te stellen dat moet garanderen dat na de voorziene overgangsperiode van 3 jaar het NCB-systeem voldoet aan het vereiste niveau.

Artikel 25 vraagt geen verdere toelichting.

Artikel 26 vraagt geen verdere toelichting.

In **artikel 27** is voorzien dat de exploitanten met netwerk- en informatiesystemen ingedeeld in Cyber-4 ten laatste 24 maanden

externes moeten worden uitgevoerd door organisaties die hiervoor geaccrediteerd zijn.

Cette accréditation doit être décernée par un organisme national d'accréditation et doit couvrir le niveau de sécurité qui fait l'objet de l'audit. Cette autorité est visée dans la loi NIS2. Une fois accréditée, l'organisation en charge de l'audit doit également être agréée par le CCB.

L'article 24 ne demande pas de commentaire particulier.

Le **chapitre IX** porte sur les dispositions transitoires pour les exploitants qui tombent sous l'application du présent projet d'arrêté et qui, au moment de l'entrée en vigueur de ce projet d'arrêté, sont déjà autorisés ou agréés par l'Agence. Ces dispositions transitoires s'appliquent également aux exploitants dont l'installation nucléaire ou l'entreprise de transport nucléaire dispose déjà d'un système de protection physique ou d'un système générique de sécurité agréé. Une période de transition est accordée à ces exploitants pour leur laisser le temps de se mettre en conformité avec le présent projet d'arrêté. Le dossier de CSN doit également comprendre une auto-évaluation pour ces exploitants. Cette auto-évaluation, qui peut également être réalisée à l'aide des outils du CCB, doit fournir un état du niveau du système de CSN existant par rapport au niveau requis. Le résultat de cette auto-évaluation doit être utilisé pour établir un plan d'action visant à garantir qu'après la période transitoire prévue de trois ans, le système de CSN atteindra le niveau requis.

L'article 25 ne demande pas de commentaire particulier.

L'article 26 ne demande pas de commentaire particulier.

L'article 27 prévoit que les exploitants de réseaux et systèmes d'information de catégorie Cyber-4 doivent, au plus tard 24

na de inwerkingtreding van dit ontwerpbesluit een NCB-systeem en de daaruit volgende nucleaire beveiligingsmaatregelen moeten hebben geïmplementeerd. Dit systeem wordt als erkend beschouwd.

Artikel 28 omvat de procedure voor de exploitanten met netwerk- en informatiesystemen die ingedeeld zijn in de categorieën Cyber 1, 2 en 3. 8 maanden na de inwerkingtreding van dit ontwerpbesluit moet een aanvraag voor de erkenning van het NCB-systeem ingediend worden. Deze periode moet de exploitanten de nodige tijd geven om het NCB-dossier op te stellen en de NCB-maatregelen voor te stellen. Na de goedkeuring van het systeem krijgen de exploitanten een maximum van 3 jaar om geleidelijk deze NCB-maatregelen te implementeren. De vooruitgang van deze implementatie wordt door het Agentschap opgevolgd via het jaarverslag.

Ik heb de eer te zijn,
Sire,
van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaar,

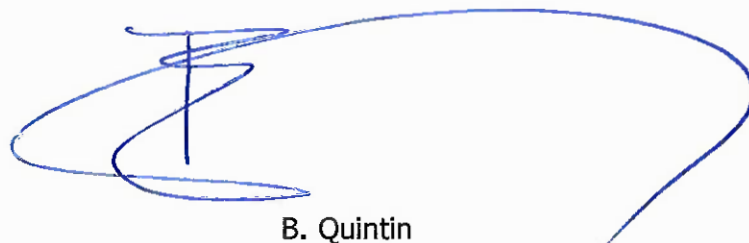
De Minister van Veiligheid en Binnenlandse Zaken, belast met Beliris

mois après l'entrée en vigueur du présent arrêté en projet, avoir mis en œuvre un système de CSN ainsi que les mesures de sécurité nucléaire qui en découlent. Ce système est considéré comme agréé.

L'article 28 décrit la procédure pour les exploitants de réseaux et systèmes d'information des catégories Cyber-1, Cyber-2 et Cyber-3. Une demande d'agrément du système de CSN doit être introduite dans les 8 mois après l'entrée en vigueur de l'arrêté. Ce délai doit permettre aux exploitants de disposer du temps nécessaire pour établir le dossier de CSN et proposer des mesures de CSN. Une fois le système approuvé, les exploitants disposent d'un maximum de trois ans pour mettre progressivement en œuvre ces mesures de CSN. L'Agence surveille l'état d'avancement de cette mise en œuvre grâce aux rapports annuels.

J'ai l'honneur d'être,
Sire,
de Votre Majesté,
le très respectueux
et très fidèle serviteur,

Le Ministre de la Sécurité et de l'Intérieur, également chargé de Beliris



B. Quintin