KONINKRIJK BELGIË	ROYAUME DE BELGIQUE
Federaal Agentschap voor Nucleaire Controle	**Agence fédérale de Contrôle nucléaire**
VERSLAG AAN DE KONING, Sire, Dit ontwerp van koninklijk besluit wordt genomen in uitvoering van artikel 17*sexies* 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 de Nucleaire Controle. Dit ontwerp van koninklijk besluit regelt in het bijzonder de in de eerste paragraaf van voormeld artikel 17*sexies* voorziene vier machtigingen voor de Koning om de nucleaire cyberbeveiligingsmaatregelen te bepalen die aan de exploitanten worden opgelegd. Er moet aan herinnerd worden dat het nucleaire cyberbeveiliging, zoals gedefinieerd in artikel 1 van de wet van 15 april 1994, niet enkel de cyberbeveiliging in nucleaire installaties en inrichtingen maar eveneens de cyberbeveiliging in de inrichtingen waar er radioactieve stoffen aanwezig zijn. (de term “nucleaire installatie” moet begrepen worden in de zin van artikel 1bis van de wet van 15 april 1994 en de term inrichting zoals bedoeld in artikel 2, 3°) van het algemeen reglement). Artikel 1 bevat de definities van een aantal begrippen die in het ontwerp van koninklijk besluit worden gebruikt. Dit artikel moet daarom samen gelezen worden met de bestaande wettelijke definities zoals deze van “netwerk- en informatiesysteem”, “cyberincident” en “cyberrisico” (die overeenkomen met de definities in de [NIS-Wet]). 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 informatiesystemen van de betrokken installaties en inrichtingen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de	RAPPORT AU ROI, Sire, Le présent projet d'arrêté royal est pris en exécution de l'article 17*sexies* 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. Le présent projet d'arrêté royal règle notamment les quatre compétences visées au § 1er de l'article 17*sexies* qui habilitent le Roi à déterminer les mesures de cybersécurité nucléaire imposées aux exploitants. Il convient de rappeler ici que la cybersécurité nucléaire, telle qu’ 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 (le terme « installation nucléaire » est à prendre au sens de l’article 1ier bis de la loi du 15 avril 1994, et le terme « établissement » au sens de l’article 2, 3°), du Règlement général) . L'article 1er contient les définitions de plusieurs termes utilisés dans le projet d'arrêté royal. Cet article doit donc être lu conjointement avec les définitions légales existantes, telles que celles de « réseau et système d'information », de « cyber-incident » et de « cyber-risque » (qui correspondent d’ailleurs aux définitions de la [loi NIS]). Les définitions de « cybersécurité nucléaire » et de « mesures de cybersécurité nucléaire » figurent à l’article 1ier 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 des installations et des établissements visés, de résister à 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

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.	d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.
Artikel 2 preciseert de netwerk- en informatiesystemen die tot het toepassingsgebied van de nucleaire cyberbeveiliging van installaties en inrichtingen behoren. Dit ontwerpbesluit 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. In dit artikel wordt eveneens voorzien dat exploitanten waarvan de netwerk- en informatiesystemen vallen onder het toepassingsgebied van de NISII richtlijn, omgezet in de wet van xx/xx/2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en de uitvoeringsbesluiten van deze wet, niet aan verschillende bepalingen van dit ontwerpbesluit onderhevig zijn, inclusief de verplichtingen met betrekking tot de erkenning door het federaal Agentschap voor Nucleaire controle. De cyberbeveiliging van hun netwerk- en informatiesystemen dienen te gebeuren conform de NIS2 wet.	L'article 2 précise les réseaux et systèmes d'information qui relèvent du champ d'application de la cybersécurité nucléaire des installations et établissements. Le présent projet d'arrêté ne s'applique pas aux réseaux et systèmes d'information des établissements qui comportent uniquement des appareils émettant des rayonnements ionisants ne provenant pas de substances radioactives. Cet article dispose également que les exploitants dont les réseaux et systèmes d'information relèvent du champ d'application de la directive NIS2 transposée dans la loi du xx/xx/2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et ses arrêtés d'exécution ne sont pas soumis aux diverses obligations du présent projet d'arrêté, ce qui inclut les obligations relatives à l'agrément par l'Agence fédérale de Contrôle nucléaire. La cybersécurité de leurs réseaux et systèmes d'information doit être assurée conformément à la loi NIS2.
Artikel 3 voorziet de indeling in categorieën van voormelde netwerk- en informatiesystemen op basis van de kritieke aard van die systemen en de al dan niet nucleaire aard van desbetreffende inrichtingen en installaties alsook de hieraan verbonden cyberrisico's. Er wordt een onderscheid gemaakt tussen vijf categorieën van netwerk- en informatiesystemen, waarvan de eerste 2 categorieën, systemen betreffen in de nucleaire sector terwijl de andere systemen in sectoren voorkomen waar er met radioactieve stoffen gewerkt worden. Dit kan zowel de medische als de industriële sector zijn. Er wordt gekeken naar systemen die zich bevinden in ofwel de veiligheidszones gedefinieerd voor kernmaterialen ofwel in de	L'article 3 prévoit la répartition en catégories des réseaux et systèmes d'information susmentionnés en fonction du caractère critique de ces réseaux et systèmes et de la nature nucléaire ou non nucléaire des établissements et installations concernés, ainsi que des cyber-risques qui y sont associés. L'article distingue cinq catégories de réseaux et systèmes d'information, dont les deux première catégories concernent des systèmes du secteur nucléaire, tandis que les autres systèmes se retrouvent dans des secteurs où sont utilisées des substances radioactives, comme le secteur médical ou le secteur industriel. Sont ici visés les systèmes qui se trouvent soit dans des zones de sécurité définies pour les

beveiligde ruimte gedefinieerd voor radioactieve stoffen, alsook de netwerk – en informatiesystemen die op enigerwijze communiceren of verbonden zijn met deze zones of ruimtes. Het betreft ook alle soorten van systemen zowel de systemen die instaan voor de informatietechnologie (IT), als deze voor de operationale technologie (OT), als IOT systemen (Internet of things). IT omvat alle technologieën die gebruikt wordt om informatie te verzamelen, op te slaan, te verwerken en te communiceren, zoals bvb: 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), Distributie Controle systemen (DCS), en Programmable Logic Controllers (PLC's). OT is cruciaal voor de werking van kritieke infrastructuur, zoals energiecentrales, waterzuiveringsinstallaties, transportsystemen, beheer pijpleidingen, enz.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 cloud applicaties gebeuren. Voorbeelden hier zijn een slimme thermostaat die de temperatuur kan regelen, slimme verlichting, sensoren die de uitlaat in schoorstenen monitoren, sensoren op apparaten voor onderhoudsplanning, … .. 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. Binnen beveiligingsniveau A moeten de essentiële nucleaire cyberbeveiligingsmaatregelen worden genomen. Binnen beveiligingsniveau B de belangrijke nucleaire	matières nucléaires, soit dans des espaces sécurisés 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. Il couvre également 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). L'OT est crucial pour le fonctionnement des infrastructures critiques, telles que les centrales électriques, les usines de traitement de l'eau, les systèmes de transport, les pipelines de gestion, etc. 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 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. 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

cyberbeveiligingsmaatregelen. Binnen beveiligingsniveau C de basis nucleaire cyber beveiligingsmaatregelen. 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. In het verdere verloop van dit besluit zullen dan ook geen verdere verplichtingen opgelegd worden voor dit beveiligingsniveau.	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. Par conséquent, dans la suite du présent projet d'arrêté, aucune autre obligation ne sera imposée pour ce niveau de sécurité.
Artikel 5 bepaalt welke van de in hoofdstuk III bepaalde maatregelen voor de 3 hoogste beveiligingsniveaus van toepassing zijn. Het tweede lid van de drie eerste paragrafen bepaalt elke keer dat het agentschap een technisch reglement kan opstellen om de opgelegde maatregelen verder te detailleren.. Deze technische reglementen zullen gebaseerd worden op de aanbevelingen van het CCB opgenomen in het cyberfundamentals framework en de aanbevelingen van het IAEA. Deze technische reglementen zullen rekening houden met een graduele aanpak voor elk van de niveaus alsook met de snelle technische vooruitgang van de sector.	L'article 5 précise les mesures définies au chapitre III qui s'appliquent aux 3 niveaux de sécurité les plus élevés. Le deuxième alinéa des trois premiers paragraphes indique chaque fois que l'Agence peut établir un règlement technique pour préciser les mesures imposées. Ces règlements techniques s'appuieront sur les recommandations du CCB qui figurent dans le cyberfundamentals framework et sur les recommandations de l'AIEA. Ces règlements techniques respecteront une approche graduée pour chacun des niveaux et tiendront compte de la rapidité de l'évolution technique dans le secteur.
Artikel 6 bevat de algemene principes inzake nucleaire cyberbeveiliging, het nemen van passende maatregelen en het door de exploitant op te stellen nucleair cyberbeveiligingsbeleid. De eerste paragraaf van artikel 6 verplicht iedere exploitant van een inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in de eerste 4 categorieën om een nucleair cyberbeveiligingsbeleid in te voeren en en continue te verbeteren. Belangrijk hier is aan te halen dat als er in het verdere verloop van dit ontwerpbesluit verplichtingen opgelegd worden aan een exploitant, er bedoeld wordt alle exploitanten ~~met~~ waarvan de netwerk- en informatiesystemen ingedeeld zijn in een van de 4 hoogste categorieën. Indien bepalingen niet van toepassing zijn op al deze exploitanten zal dit expliciet vermeld worden. De tweede paragraaf van artikel 6 schrijft in algemene termen voor dat de exploitant de	L'article 6 concerne les principes généraux en matière de cybersécurité nucléaire, la prise de mesures appropriées et la politique de cybersécurité nucléaire que doit établir l'exploitant. Le premier paragraphe de l'article 6 oblige chaque exploitant d'un établissement dont les réseaux et systèmes d'information sont classés dans l'une des 4 premières catégories à établir et d'améliorer en continue une politique de cybersécurité nucléaire. Il est important de souligner que lorsque des obligations sont imposées à un exploitant dans les dispositions suivantes du projet d'arrêté, elles s'appliquent à tous les exploitants dont les réseaux et systèmes d'information sont classés dans l'une des 4 catégories les plus élevées. Si les dispositions ne s'appliquent pas à tous ces exploitants, l'arrêté le précise explicitement. Le deuxième paragraphe de l'article 6 dispose en termes généraux que l'exploitant doit prendre

passende maatregelen moet nemen rekening houdend met de stand van de technische kennis en afgestemd op de cyberrisico's die zich voordoen alsook gekoppeld aan het beveiligingsniveau en de binnen dit niveau voorgeschreven cyberbeveiligingsmaatregelen. In dit verband wordt naar het voorbeeld van andere wetgeving inzake gegevensbescherming en informatieveiligheid, zoals [NIS-Wet] en [AVG] een risico-gebaseerde benadering gehanteerd waarbij de exploitant de cyberrisico's moet beheersen en cyberincidenten moet voorkomen of de impact ervan moet beperken, rekening houdend met de technische kennis en de evolutie ervan.	les mesures appropriées en tenant compte de l'état des connaissances techniques, des cyber-risques présents, du niveau de sécurité et des mesures de cybersécurité prescrites pour ce niveau. Sur le modèle d'autres législations relatives à la protection des données et à la sécurité de l'information, telles que la [loi NIS] et le [RGPD], le projet d'arrêté royal prône une approche par les risques, selon laquelle l'exploitant doit maîtriser les cyber-risques et prévenir les cyber-incidents ou en limiter l'impact, en tenant compte des connaissances techniques et de leur évolution.
De derde paragraaf van artikel 6 voorziet in het nemen van mogelijke bijkomende nucleaire cyberbeveiligingsmaatregelen door de exploitant wanneer deze kennis heeft van een specifieke dreiging tegen zijn inrichting, zijn installatie of zijn netwerk- en informatiesystemen.	Le troisième paragraphe de l'article 6 prévoit que l'exploitant doit prendre des mesures de cybersécurité nucléaire supplémentaires lorsqu'il a connaissance d'une menace spécifique à l'encontre de son établissement, de son installation ou de ses réseaux et systèmes d'information.
De vierde paragraaf van artikel 6 vloeit voort uit de algemene cyberbeveiligingsplicht van de eerste twee paragrafen en schrijft voor dat de exploitant werk moet maken van een gedocumenteerd cyberbeveiligingsbeleid dat moet voldoen aan de voorwaarden van afdeling III van dit ontwerp van koninklijk besluit. Dit impliceert dat de exploitant, naast een gedocumenteerde omschrijving van de door hem te nemen cyberbeveiligingsmaatregelen, zijn netwerk- en informatiesystemen in kaart moet brengen en de kritieke aard ervan en de toepasselijke in artikelen 3 en 4 van dit ontwerp voorziene categorieën en overeenstemmende beveiligingsniveaus moet vaststellen om vervolgens een analyse te maken van de cyberrisico's en mogelijke cyberincidenten, de kans dat deze risico's zich zullen voordoen, de ernst ervan, de omvang, de context etc. Overeenkomstig de vijfde paragraaf van artikel 6 moet de exploitant voor de opmaak van het gedocumenteerd cyberbeveiligingsbeleid advies inwinnen van de afgevaardigde voor cyberbeveiliging (zie verder onder artikel 7 van dit ontwerp). In paragraaf 6 wordt de minimale inhoud van dit cyberbeveiligingsbeleid opgesomd.	Le quatrième paragraphe de l'article 6 découle de l'obligation générale de cybersécurité visée aux deux premiers paragraphes et stipule que l'exploitant doit établir une politique de cybersécurité documentée qui répond aux conditions de la section III du présent projet d'arrêté royal. Concrètement, l'exploitant doit fournir une description documentée des mesures de cybersécurité qu'il doit prendre, mais il doit également schématiser ses réseaux et systèmes d'information et déterminer leur criticité ainsi que les catégories applicables et les niveaux de sécurité correspondants visés aux articles 3 et 4 du présent projet, pour ensuite procéder à une analyse des cyber-risques et des cyber-incidents potentiels, de la probabilité de la survenance de ces risques, de leur gravité, de leurs proportions, de leur contexte, etc. Conformément au cinquième paragraphe de l'article 6, l'exploitant doit solliciter l'avis du délégué à la cybersécurité pour élaborer sa politique documentée de cybersécurité (voir le commentaire de l'article 7 du présent projet). Le paragraphe 6 précise le contenu minimum de cette politique écrite de cybersécurité.

Verder bepaald dit artikel dat het nucleair cyberbeveiligingsbeleid moet geïntegreerd zijn in de managements- kwaliteits- of beheersystemen van de exploitant. De exploitant staat uiteraard ook in voor de nodige vorming van zijn personeel en in het bijzonder die van de afgevaardigde voor cyberbeveiliging. Deze afgevaardigde is, zoals verder bepaald, een belangrijke schakel in het opzetten en onderhouden van het nucleaire cyberbeveiligingsbeleid en de daarbij horende nucleaire cyberbeveiligingsmaatregelen.	Par ailleurs, cet article stipule que la politique de cybersécurité nucléaire doit être intégrée dans les systèmes de management, de qualité ou de gestion de l'exploitant. L'exploitant est, bien entendu, également responsable de prévoir la formation nécessaire de son personnel et, en particulier, du délégué à la cybersécurité. Ce délégué est, comme stipulé plus loin, un maillon important dans l'établissement et le maintien de la politique de cybersécurité nucléaire et des mesures de cybersécurité nucléaire qui en découlent.
De exploitant moet zijn beleid en de beveiliging van zijn netwerk- en informatiesystemen op periodieke basis auditeren en laten auditeren. Rekening houdend met een graduele aanpak zijn de frequenties van de audits verschillend voor de verschillende categorieën. De externe audits moeten uitgevoerd worden door organisaties die daarvoor geaccrediteerd zijn. Deze accreditatie dient te gebeuren door de nationale accreditatieautoriteit, deze moet geldig zijn voor het beveiligingsniveau dat aan de audit wordt onderworpen. Deze autoriteit is voorzien in de wet van xx/xx/2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS2 wet). Na de accreditatie moet de auditorganisatie ook erkend worden door het CCB.	L’exploitant doit soumettre sa politique ainsi que 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 externes doivent être réalisés par des organisations accréditées à cet effet. Cette accréditation doit être décernée par l'autorité nationale d'accréditation et doit couvrir le niveau de sécurité qui fait l’objet de l’audit. Cette autorité est visée dans la loi de xx/xx/2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d’intérêt général pour la sécurité publique (loi NIS2). Une fois accréditée, l'organisation en charge de l'audit doit également être agréée par le CCB.
Paragraaf 13 van artikel 6 is ten slotte een open bepaling op basis waarvan het Agentschap aanbevelingen of technische reglementen kan uitvaardigen met bijkomende vereisten of voorschriften inzake het cyberbeveiligingsbeleid.	Enfin, le paragraphe 13 de l'article 6 est une disposition ouverte sur la base de laquelle l'Agence peut adopter des recommandations ou des règlements techniques comportant des exigences ou des règles complémentaires en matière de politique de cybersécurité.
Artikel 7 van dit ontwerp regelt de aanstelling van een afgevaardigde voor cyberbeveiliging. Dit kan volgens de eerste paragraaf van artikel 7, afhankelijk van de structuur of organisatie van de entiteit van de exploitant, iemand binnen de organisatie zijn, zoals een werknemer of aangestelde van de exploitant, of iemand extern, zolang er een duurzame relatie is met de exploitant. Er is geen verplichting opgenomen om ook een backup afgevaardigde aan te stellen	L'article 7 du présent projet régit la désignation d'un délégué à la cybersécurité. En vertu du premier paragraphe de l'article 7, il peut s’agir, selon la structure ou l'organisation de l'entité de l’exploitant, soit d'une personne interne à l'organisation, comme un travailleur ou un préposé de l’exploitant, 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

maar in grotere ondernemingen is dit wel een goede praktijk. De exploitant moet mogelijke belangenconflicten vermijden in hoofde van de afgevaardigde voor cyberbeveiliging. Die moet naar het voorbeeld van 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 moeten worden 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 bvb de volgende 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. De aanstelling moet overeenkomstig de derde paragraaf van artikel 7 voorafgaandelijk goedgekeurd worden door het Agentschap. Indien de aangestelde afgevaardigde voor cyberbeveiliging 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. Het Agentschap kan nog aanbevelingen of een technisch reglement opstellen dat de praktische modaliteiten voor de aanstelling en goedkeuring kan opnemen. Artikel 8 van dit ontwerp van koninklijk besluit regelt de positie, rol en de taken van de afgevaardigde voor cyberbeveiliging. Het is belangrijk ~~hier~~ aan te geven dat de eindverantwoordelijkheid van de nucleaire cyberbeveiliging bij de exploitant berust. Het is de opdracht en de taak van de afgevaardigde voor cyberbeveiliging om het nucleair	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 cybersécurité. 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, formations professionnelles ou diplômes suivants : • Certified Information Systems Auditor (CISA), • Certified Information Security Manager (CISM), • Certified Information Systems Security Professional (CISSP) • un bachelier ou un master en sécurité de l'information ou en cybersécurité, ou un diplôme équivalent. La désignation doit être préalablement approuvée par l'Agence, conformément au troisième paragraphe l'article 7. Si le délégué à la cybersécurité qui a été désigné n'exerce plus cette fonction, il doit en avertir 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'Agence peut adopter des recommandations ou un règlement technique pour déterminer les modalités pratiques de la désignation et de l'approbation. L'article 8 du présent projet d'arrêté royal régit la position, le rôle et les tâches du délégué à la cybersécurité. Il est important de souligner que la responsabilité finale de la cybersécurité nucléaire incombe à l'exploitant. Il relève de la mission et des tâches du délégué à la cybersécurité de mettre en œuvre la politique de cybersécurité nucléaire et d'adopter les

cyberbeveiligingsbeleid uit te voeren en daarvoor de nodige nucleaire cyberbeveiligingsmaatregelen op te zetten maar 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 nucleaire cyberbeveiliging.	mesures de cybersécurité nucléaire 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 cybersécurité soit impliqué suffisamment et en temps utile dans toutes les questions qui touchent à la cybersécurité nucléaire.
De afgevaardigde voor cyberbeveiliging moet ook voldoende gekend zijn bij iedereen binnen de entiteit van de exploitant. Tevens moeten aan hem overeenkomstig paragraaf 2 van artikel 8 de nodige ondersteuning en middelen ter beschikking worden gesteld voor de uitoefening van zijn taken. Belangrijk hier is dat ook de nodige middelen en tijd ter beschikking gesteld wordt opdat de afgevaardigde zijn deskundigheid kan in stand houden. Gezien de snel wijzigende technologische evoluties en de steeds wijzigende cyberrisico's is dit van primordiaal belang.	Le délégué à la cybersécurité doit également être suffisamment connu de tous au sein de l'entité de l'exploitant. Il doit en outre bénéficier de l'assistance et des ressources nécessaires à l'exercice de ses tâches, en vertu du paragraphe 2 de l'article 8. Il est ici également important que le délégué à la cybersécurité dispose des ressources et du temps nécessaires pour entretenir son expertise. C'est même primordial si l'on considère la rapidité des évolutions technologiques et la constante mutation des cyber-risques.
Paragraaf 3 schrijft voor dat de afgevaardigde voor cyberbeveiliging rechtstreeks verslag dient uit te brengen aan de hoogste leidinggevende van de exploitant. Paragraaf 4 van artikel 8 omschrijft één van de meest essentiële taken van de afgevaardigde voor cyberbeveiliging, namelijk het informeren en adviseren van de exploitant en zijn medewerkers over alles wat met nucleaire cyberbeveiliging te maken heeft, zowel juridisch als technisch. De afgevaardigde voor cyberbeveiliging 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 nucleaire cyberbeveiliging van de exploitant (paragraaf 5).	Le paragraphe 3 dispose que le délégué à la cybersécurité doit dépendre directement du plus haut responsable de l'exploitant. Le paragraphe 4 de l'article 8 décrit une des tâches essentielles du délégué à la cybersécurité, qui consiste à informer et à conseiller l'exploitant et ses collaborateurs sur tout ce qui a trait à la cybersécurité nucléaire, tant sur le plan juridique que technique. Le délégué à la cybersécurité 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 cybersécurité nucléaire de l'exploitant (paragraphe 5).
De zesde paragraaf van artikel 8 omschrijft een andere essentiële taak van de afgevaardigde voor cyberbeveiliging, namelijk het toezien op de naleving van het nucleair cyberbeveiligingsbeleid van de exploitant dat door of op advies van de afgevaardigde voor cyberbeveiliging werd uitgewerkt. Naar het voorbeeld van de functionaris voor de gegevensbescherming (DPO) moet de afgevaardigde voor cyberbeveiliging het eerste contactpunt zijn inzake nucleaire cyberbeveiliging, zowel intern voor de	Le sixième paragraphe de l'article 8 décrit une autre tâche essentielle du délégué à la cybersécurité, qui consiste à contrôler le respect de la politique de cybersécurité nucléaire de l'exploitant qui a été établie par ses soins ou sur ses conseils . À l'instar du délégué à la protection des données (DPO), le délégué à la cybersécurité doit être le point de contact privilégié en matière de cybersécurité nucléaire, tant en interne pour le personnel de l'exploitant qu'en externe pour les tiers ou les autorités

medewerkers van de exploitant, als extern ten aanzien van derden of bevoegde autoriteiten en dit zonder afbreuk te doen op de verantwoordelijkheden van de exploitant.	compétentes, sans préjudice des responsabilités de l'exploitant.
De achtste paragraaf van artikel 8 kadert in de interne bewustwording onder de medewerkers van de exploitant waarbij de afgevaardigde voor cyberbeveiliging 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.	Le huitième paragraphe de l'article 8 s'inscrit dans le cadre de la conscientisation en interne du personnel de l'exploitant, le délégué à la cybersécurité 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.
Paragraaf 9 van artikel 8 sluit aan op de essentiële toezichthoudende taak van de afgevaardigde voor cyberbeveiliging met betrekking tot het door de exploitant ingestelde cyberbeveiligingsbeleid. Het niet toepassen van dit beleid moet door de afgevaardigde voor cyberbeveiliging onmiddellijk gemeld worden aan de exploitant.	Le paragraphe 9 de l'article 8 se rapporte à la tâche essentielle de contrôle du délégué à la cybersécurité par rapport à la politique de cybersécurité instaurée par l'exploitant. Le non-respect de cette politique doit être immédiatement communiqué par le délégué à la cybersécurité à l'exploitant.
Paragraaf 10 van artikel 8 voorziet in de verplichting voor de afgevaardigde voor cyberbeveiliging 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.	Le paragraphe 10 de l'article 8 prévoit l'obligation pour le délégué à la cybersécurité 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.
Niet onbelangrijk is paragraaf 11 waar er expliciet opgenomen is dat de afgevaardigde zich kan laten bijstaan of advies kan inwinnen bij externe partijen. In een snel veranderende hoogtechnologische omgeving is het vaak noodzakelijk om bijkomende expertise te raadplegen.	Le paragraphe 11 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.
Artikelen 9 tot en met 13 bevatten een vrij uitvoerige lijst van nucleaire cyberbeveiligingsmaatregelen die gebaseerd is op het CCB Cyberfundamentals Framework waarbij ook rekening werd gehouden met de relevante inzichten opgenomen in andere normen of kaders inzake informatieveiligheid en/of cyberbeveiliging zoals NIST/CFS, ISO 27001/ISO 27002, IEC 62443 en de CIS Controls (ETSI TR 103 305-1).	Les articles 9 à 13 énumèrent de manière relativement exhaustive les mesures de cybersécurité nucléaire qui se basent sur le Cyberfundamentals Framework du CCB et qui ont été définies en tenant compte des idées pertinentes qui sous-tendent d'autres normes ou cadres relatifs à la sécurité de l'information et/ou à la cybersécurité tels que NIST/CFS, ISO 27001/ISO 27002, IEC 62443 et les CIS Controls (ETSI TR 103 305-1).
Voormelde artikelen zijn opgebouwd rond de vijf kernprincipes binnen de informatieveiligheid en cyberbeveiliging: 1. **Identificeren** (artikel 9) met onder meer de verplichting voor de exploitant om de	Les articles susmentionnés s'articulent autour des cinq principes fondamentaux de la sécurité de l'information et de la cybersécurité : 1. **Identifier** (article 9), ce qui concerne notamment l'obligation pour l'exploitant

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 beheren en kwetsbaarheden te identificeren. Ook de gegevens en informatiestromen moeten in kaart gebracht worden gedocumenteerd worden en continu bijgewerkt. Het documenteren van deze gegevensstromen houdt ook in dat deze stromen 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, tijd, personeel, software, … Wanneer het gaat over het bepalen van de cyberrisico's in de toeleveringsketen is het aan te 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.	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 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, le temps, le personnel, 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.
2. **Beschermen** (artikel 10) met onder meer de verplichting om de toegang tot systemen te beheren, authenticatieniveaus te bepalen, netwerken en applicaties af te schermen, opleidingen inzake cyberbeveiliging 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, … kunnen in gedrang brengen. Gevoelige gegevens kunnen bvb deze gegevens zijn die omwille van andere regelgevingen moeten beschermd worden of die zich in de privé sfeer bevinden.	2. **Protéger** (article 10), ce qui concerne notamment l'obligation de gérer l'accès aux systèmes, de déterminer les niveaux d'authentification, de protéger les réseaux et les applications, d'organiser des formations en cybersécurité, 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.

3. **Detecteren** (artikel 11) 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 als dat van externe binnen het netwerk- en informatiesysteem heeft als doel abnormaliteiten te detecteren die mogelijk schade kunnen berokkenen.	3. **Détecter** (article 11), ce qui implique 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.
4. **Reageren en herstellen** (artikel 12) met de 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 alzo de beveiliging van de netwerk- en informatiesystemen te verbeteren.	4. **Répondre et rétablir** (article 12), ce qui couvre les obligations et les mesures à prendre pour répondre aux cyber-incidents, les signaler, 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.
5. **Testen** (artikel 13) met verplichtingen om het nucleair cyberbeveiligingsbeleid periodiek te testen. Dit testen dient met een zekere regelmaat te gebeuren zodat de meest recente tactieken en aanval scenario's kunnen toegepast worden. 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 daar naar vraagt. Indien het de bijkomende maatregelen van die aard zijn dat het nucleair cyberbeveiligingsbeleid dient aangepast te worden, kan deze evaluatie deel uitmaken van de aanvraag tot wijziging van de erkenning van dit beleid.	5. **Tester** (article 13), ce qui concerne les obligations de tester périodiquement la politique de cybersécurité nucléaire. Ces tests doivent être réalisés avec une certaine régularité de sorte qu'ils puissent tenir compte des tactiques et des scénarios d'attaque les plus récents. 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. Si les mesures supplémentaires sont de nature à requérir la modification de la politique de cybersécurité nucléaire, cette évaluation peut faire partie de la demande de modification de l'agrément de cette politique.
Artikel 14 bevat de meldingsplicht voor exploitanten met betrekking tot cyberincidenten die significante gevolgen	L'article 14 porte sur l'obligation pour les exploitants de notifier les cyber-incidents ayant un impact significatif sur la disponibilité, la

hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van hun netwerk- en informatiesystemen. Dit is naar het voorbeeld van andere wettelijke meldingsplichten zoals voorzien in de [NIS II-Wet] voor incidenten en 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 95/46/EG (algemene verordening gegevensbescherming) voor risicovolle inbreuken in verband met persoonsgegevens en de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.	confidentialité, l'intégrité ou l'authenticité de leurs réseaux et systèmes d'information. Cette disposition s'appuie sur le modèle d'autres obligations légales de notification comme celles de la [loi NIS 2] pour les incidents, du 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 (règlement général sur la protection des données) pour les violations de données à caractère personnel, et de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
Bij het beoordelen of een incident significante gevolgen heeft moeten verschillende parameters in rekening gebracht worden. O.a. de mogelijke impact op de onderneming maar wat zeker belangrijk is om te evalueren zijn de gevolgen waardoor een veilige en beveiligde uitbating van de inrichting of installatie niet langer gegarandeerd kan worden.	Plusieurs paramètres entrent en ligne de compte pour déterminer si un incident a un impact significatif. L'impact potentiel sur l'entreprise doit certes être déterminé, mais ce qu'il est surtout important d'évaluer, ce sont les implications qui entraîneraient l'impossibilité de garantir l'exploitation sure et sécurisée de l'établissement ou de l'installation.
Overeenkomstig de eerste paragraaf van artikel 14 moet de exploitant dergelijke cyberincidenten onmiddellijk (zo snel mogelijk) melden aan Agentschap. De tweede paragraaf bepaalt dat de exploitant waarvan de netwerk- en informatiesystemen ingedeeld zijn in het hoogste beveiligingsniveau ook rechtstreeks moet melden aan het cyber security Early Warning Systeem.	Conformément au premier paragraphe de l'article 14, l'exploitant doit notifier immédiatement (dans les meilleurs délais) ces cyber-incidents à l'Agence. Le deuxième paragraphe stipule que l'exploitant dont les réseaux et systèmes d'information sont catégorisé au niveau de sécurité le plus élevé doit aussi directement notifier ces cyber-incidents dans le Cyber Security Early Warning System.
De derde paragraaf van artikel 14 schrijft voor wat minimum moet worden meegedeeld bij een dergelijke melding, zoals de aard van het cyberincident, de betrokken netwerk- en informatiesystemen, de overeenkomstig artikel 3 van dit ontwerp vastgestelde categorieën, de contactgegevens van de afgevaardigde voor cyberbeveiliging of een ander contactpunt van de exploitant, de waarschijnlijke gevolgen van het cyberincident en de risico beperkende maatregelen die reeds werden en/of nog zullen worden genomen door de exploitant. Ook	Le troisième paragraphe de l'article 14 prescrit ce qui doit être au moins communiqué lors d'une telle notification, comme la nature du cyber-incident, les réseaux et systèmes d'information impactés, les catégories définies en vertu de l'article 3 du présent projet, les coordonnées du délégué à la cybersécurité de l'exploitant ou d'un autre point de contact, les incidences probables du cyber-incident et les mesures visant à limiter les risques qui ont déjà été prises et/ou qui seront prises par l'exploitant. Ici aussi, un rôle important est dévolu au délégué à la cybersécurité.

hierbij is een belangrijke rol weggelegd voor de afgevaardigde voor cyberbeveiliging. De vierde paragraaf van artikel 14 schrijft voor dat de exploitant alle cyberincidenten moet documenteren in een incidentenregister dat zo nodig ter beschikking moet worden gehouden van het Agentschap.	Le quatrième paragraphe de l'article 14 dispose que l'exploitant doit documenter tous les cyber-incidents dans un registre des incidents qui doit être tenu à la disposition de l'Agence, en cas de besoin.
Artikel 15, eerste paragraaf van dit ontwerp van koninklijk besluit regelt de adequate uitwisseling van informatie over cyberrisico's of cyberincidenten waarmee exploitanten worden geconfronteerd tussen de reeds hierboven vermelde autoriteiten (het Agentschap, CCB en NCCN). De doelstelling hiervan is om het mogelijk te maken dat deze autoriteiten op het gebied van cyberbeveiliging, de kritieke infrastructuren of het crisisbeheer hun medewerking, advies en ervaring ter beschikking kunnen stellen van de nucleaire cyberbeveiliging. In de tweede paragraaf van artikel 15 wordt verduidelijkt dat die informatie-uitwisseling moet worden afgewogen tegenover de veiligheid en de belangen van de exploitanten. 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 95/46/EG (algemene verordening gegevensbescherming).	L'article 15, premier paragraphe, du présent projet d'arrêté royal régit l'échange entre les autorités susmentionnées (l'Agence, le CCB et la DGCC) des informations sur les cyber-risques ou cyber-incidents auxquels sont confrontés les exploitants. L'objectif est que ces autorités compétentes dans les domaines de la cybersécurité, des infrastructures critiques ou de la gestion de crise puissent mettre leur collaboration, leurs conseils et leur expérience au service de la cybersécurité nucléaire. Le deuxième paragraphe de l'article 15 précise que cet échange d'informations doit être mis en balance avec la sûreté et les intérêts des exploitants. En outre, cet échange doit respecter 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 (règlement général sur la protection des données).
Hoofdstuk VII bevat de bepalingen voor wat betreft de erkenningsprocedure van de nucleaire cyberbeveiligingsmaatregelen. De erkenning van de maatregelen zal verlopen via een erkenning van het nucleair cyberbeveiligingsbeleid. Gezien de snelle technologische evolutie van de sector en de maatregelen die genomen kunnen/moeten worden is er voor gekozen de erkenning te baseren op het beleid waarin de grote principes van de te nemen maatregelen moeten opgenomen zijn. Dit zorgt voor meer stabiliteit in de erkenning en vermijdt een veelvuldig wijzigingsproces van een erkenning van de specifieke beveiligingsmaatregelen.	Le chapitre VII contient les dispositions relatives à la procédure d'agrément des mesures de cybersécurité nucléaire. L'agrément décerné ne porte pas sur des mesures de cybersécurité nucléaire, mais bien sur la politique de cybersécurité nucléaire. Compte tenu de l'évolution rapide de la technologie dans le secteur et des mesures qui peuvent/doivent être prises, il a été choisi d'agréer la politique dans laquelle doivent figurer les grands principes des mesures à prendre. Le but de ce choix est de garantir une plus grande stabilité au niveau de l'agrément et d'éviter une multitude de modifications d'un agrément qui porterait sur des mesures de sécurité spécifiques.

Dit hoofdstuk behandelt het proces voor nieuwe exploitanten en houdt ook rekening met de graduele aanpak. Voor exploitanten die reeds actief zijn (vergund volgens de bepalingen van het algemeen reglement) zijn er verder in dit ontwerp overgangsmaatregelen gedefinieerd. De exploitanten die een nucleair cyberbeveiligingsbeleid moeten opstellen zijn diegene die ook fysieke beveiligingsmaatregelen voor de radioactieve stoffen of de kernmaterialen moeten nemen. Dit volgens de bepalingen van KB-RAMAS of de KB's van 2011. Artikel 16 bepaalt welke exploitanten een erkenning moeten aanvragen. Artikel 17 werd ingevoegd om duidelijkheid te geven wat de exploitant moet doen indien er binnen de inrichting netwerk- en informatiesystemen aanwezig zijn die ingedeeld kunnen worden in verschillende beveiligingsniveaus. In dat geval zal de exploitant alle systemen moeten beveiligen volgens het hoogste niveau 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 kan dit aantonen kan de exploitant het lagere beveiligingsniveau aanhouden. Artikel 18 omvat de procedure voor de erkenning van het nucleair cyberbeveiligingsbeleid voor netwerk- en informatiesystemen ingedeeld in de categorie Cyber-4. In dit geval moet het nucleair cyberbeveiligingsbeleid toegevoegd worden aan het beveiligingsplan dat eveneens moet ingediend worden in het kader van het KB van xx xx 2024 betreffende de beveiliging van radioactieve stoffen en bepaalde kernmaterialen. Deze koppeling laat het Agentschap toe zowel de "fysieke" beveiliging van de radioactieve stoffen als de virtuele component samen te evalueren. De implementatie van zowel de fysieke beveiliging als de virtuele moeten gebeurd zijn alvorens de exploitant zijn installatie of inrichting kan opstarten.	Ce chapitre traite de la procédure pour les nouveaux exploitants et intègre l'approche graduée. Pour les exploitants déjà en activité (autorisés en vertu des dispositions du règlement général), des mesures transitoires sont définies plus loin dans le présent projet. Les exploitants qui doivent établir une politique de cybersécurité nucléaire sont ceux qui doivent également prendre des mesures de protection physique à l'égard de substances radioactives ou de matières nucléaires, conformément aux dispositions de l'AR RAMAS ou des AR de 2011. L'article 16 détermine les exploitants qui doivent solliciter un agrément. L'article 17 a été inséré pour clarifier ce que l'exploitant doit faire si l'établissement comporte des réseaux et systèmes d'information qui peuvent être classés dans des niveaux de sécurité différents. Dans ce cas, l'exploitant devra sécuriser tous les systèmes selon le niveau le plus élevé 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. L'article 18 décrit la procédure d'agrément de la politique de cybersécurité nucléaire pour les réseaux et systèmes d'information classés dans la catégorie Cyber-4. Dans ce cas, la politique de cybersécurité nucléaire doit être jointe au plan de sécurité qui doit également être soumis en vertu de l'arrêté royal du xx xx 2024 relatif à la sécurité des substances radioactives et de certaines matières nucléaires. Cette combinaison permet à l'Agence d'évaluer conjointement la sécurité « physique » des substances radioactives et la sécurité de la composante virtuelle. La mise en œuvre de la protection physique et de la protection virtuelle doit être effective avant que l'exploitant ne puisse démarrer son installation ou son établissement.

Artikel 19 bepaalt de procedure voor exploitanten die netwerk- en informatiesystemen hebben ingedeeld in de Cyber-3 categorie. Ook dit erkenningsproces wordt uitgevoerd gelijktijdig met het erkenningsproces voorzien in het kader van het KB van xx xx 2024 betreffende de beveiliging van radioactieve stoffen en bepaalde kernmaterialen.	L'article 19 définit la procédure d'agrément pour les exploitants qui possèdent des réseaux et systèmes d'information classés dans la catégorie Cyber-3. Ici aussi, cette procédure d'agrément s'effectue parallèlement à la procédure d'agrément visée dans l'arrêté royal du xx xx 2024 relatif à la sécurité des substances radioactives et de certaines matières nucléaires.
Artikel 20 bepaalt de procedure voor exploitanten die netwerk- en informatiesystemen hebben ingedeeld in de Cyber-2 en cyber 1 categorie. Dit erkenningsproces wordt uitgevoerd gelijktijdig met de aanvraag tot het bekomen van de erkenning van het fysiek beveiligingssysteem van zijn installatie volgens de bepalingen van artikel 8 §1 van het Koninklijk besluit van 17 oktober 2011 betreffende de fysieke beveiliging van het kernmateriaal en de nucleaire installaties	L'article 20 définit la procédure d'agrément pour les exploitants qui possèdent des réseaux et systèmes d'information classés dans les catégories Cyber-2 et Cyber-1. Cette procédure s'effectue parallèlement à la procédure de traitement d'une demande d'agrément pour le système de protection physique de l'installation, introduite conformément aux dispositions de l'article 8 §1 de l'arrêté royal du 17 octobre 2011 relatif à la protection physique des matières et installations nucléaires.
Artikel 21 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.	L'article 21 traite des modifications apportées aux réseaux et systèmes d'information. Eu 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.
Artikel 22 verplicht het Agentschap om bij de evaluatie en beoordeling van de ingediende erkenningsdossiers rekening te houden met de snelle technische evolutie in het domein.	L'article 22 oblige l'Agence à tenir compte de l'évolution rapide des techniques dans le domaine lors de l'évaluation et de l'examen des dossiers d'agrément introduits.
Artikel 22bis werd specifiek toegevoegd om het Agentschap toe te laten bij het opstellen van de technische reglementen rekening te houden met aanbevelingen die door het CCB gepubliceerd en up-to-date gehouden worden. Hoofdstuk VIII behandelt de overgangsbepalingen voor klasse II en III exploitanten die onder toepassing van dit ontwerp besluit vallen en op het ogenblik van de inwerkingtreding van dit besluit reeds vergund zijn volgens de bepalingen van artikel 7 en 8 van het algemeen reglement. Alsook op de klasse I exploitanten die reeds een erkend fysiek beveiligingssysteem hebben volgens artikel 8 §1	L'article 22bis a été inséré spécifiquement pour permettre à l'Agence de prendre en compte les recommandations publiées et tenues à jour par le CCB lorsqu'elle établit les règlements techniques. Le chapitre VIII porte sur les dispositions transitoires pour les exploitants de classes II et III 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 en vertu des dispositions des articles 7 et 8 du règlement général. Ces dispositions transitoires s'appliquent également aux exploitants de classe I qui disposent déjà d'un système de

van het Koninklijk besluit van 17 oktober 2011 betreffende de fysieke beveiliging van het kernmateriaal en de nucleaire installaties. Voor deze exploitanten wordt een overgangsperiode voorzien zodat zij de tijd krijgen zich in regel te stellen met dit ontwerpbesluit. In artikel 24 is voorzien dat de exploitanten met netwerk- en informatiesystemen ingedeeld in Cyber-4 ten laatste 24 maanden na de inwerkingtreding van dit ontwerpbesluit een nucleair cyberbeveiligingsbeleid en de daaruit volgende nucleaire beveiligingsmaatregelen moeten geïmplementeerd hebben. Dit beleid wordt automatisch erkend. Na deze 24 maanden zal het Agentschap via inspecties verifiëren of de genomen nucleaire cyberbeveiligingsmaatregelen voldoen aan de bepalingen van dit ontwerp besluit. Artikel 25 omvat de procedure voor de exploitanten die netwerk- en informatiesystemen bezitten die ingedeeld zijn in de categorieën cyber 1, 2 en 3. 18 maanden na de inwerkingtreding van dit ontwerpbesluit moet een aanvraag voor de erkenning van het nucleair cyberbeveiligingsbeleid ingediend worden. Deze periode moet de exploitanten de nodige tijd geven om dit beleid op te stellen en de nucleaire cyberbeveiligingsmaatregelen voor te stellen. Na de goedkeuring van dit beleid krijgen de exploitanten een maximum van 3 jaar om geleidelijk deze cyberbeveiligingsmaatregelen te implementeren. De vooruitgang van deze implementatie wordt door het Agentschap opgevolgd via het jaarverslag.	protection physique agréé en vertu de l'article 8, §1ier de l'arrêté royal du 17 octobre 2011 relatif à la protection physique des matières nucléaires et des installations nucléaires. 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. L'article 24 prévoit que les exploitants qui possèdent des réseaux et systèmes d'information classés dans la catégorie Cyber-4 doivent, au plus tard 24 mois après l'entrée en vigueur du présent projet d'arrêté, avoir implémenté une politique de cybersécurité nucléaire ainsi que les mesures de sécurité nucléaire qui en découlent. Cette politique est automatiquement agréée. Au terme de ces 24 mois, l'Agence vérifie par des inspections si les mesures de cybersécurité nucléaire adoptées sont conformes aux dispositions du présent projet d'arrêté. L'article 25 décrit la procédure pour les exploitants qui possèdent des réseaux et systèmes d'information classés dans les catégories Cyber-1, Cyber-2 et Cyber-3. Une demande d'agrément de la politique de cybersécurité nucléaire doit être introduite dans les 18 mois après l'entrée en vigueur du présent projet d'arrêté. Ce délai doit permettre aux exploitants de disposer du temps nécessaire pour établir cette politique et proposer des mesures de sécurité nucléaire. Une fois cette politique approuvée, les exploitants disposent d'un maximum de trois ans pour mettre progressivement en œuvre ces mesures de cybersécurité. L'Agence surveille l'état d'avancement de cette mise en œuvre grâce aux rapports annuels.