Formulář k zasílání připomínek k návrhu nového zákona o kybernetické bezpečnosti a souvisejících předpisů ze strany odborné veřejnosti

Návrh nového zákona o kybernetické bezpečnosti a souvisejících předpisů naleznete ZDE.

NÚKIB upozorňuje, že:

- proces připomínkování návrhu nového zákona o kybernetické bezpečnosti a souvisejících předpisů nenahrazuje meziresortní připomínkové řízení ani žádnou jinou část legislativního procesu, jehož zahájení je plánováno na polovinu roku 2023,
- zveřejněné návrhy nového zákona o kybernetické bezpečnosti a souvisejících předpisů jsou návrhy NÚKIB a lze předpokládat, že budou v souvislosti s připomínkami i následným legislativním procesem měněny (z tohoto důvodu také není nutné připomínkovat formátování, ani další textové úpravy zveřejněných návrhů – na zveřejněné návrhy nejsou v tuto chvíli kladeny plné nároky plynoucí z Legislativních pravidel vlády),
- zasláním připomínky zasilatel potvrzuje, že byl informován o zpracování osobních údajů za účelem vypořádání připomínky, informace o zpracování osobních údajů jsou dostupné ZDE.
- vypořádání připomínky bude zasláno pouze tomu, kdo uvede své kontaktní údaje v příslušné části tohoto formuláře, jinak má Úřad za to, že zasilatel o zaslání vypořádání nemá zájem,
- připomínky budou vypořádávány v co nejkratším termínu, avšak v závislosti na dostupných kapacitách,
- má právo navrhovanou změnu odmítnout (především pokud bude rozporná se zněním směrnice NIS2), případně změnit její navrhovanou podobu při zachování původní myšlenky.

NÚKIB dále upozorňuje, že se bude připomínkami zabývat, pokud splní následující podmínky:

- návrh bude relevantní k dané problematice, bude alespoň stručně zdůvodněn a bude obsahovat základní návrh řešení,
- návrh bude ctít podmínky právního státu a principy, na kterých je postaven zákon o kybernetické bezpečnosti.
- tento formulář s návrhy bude zaslán e-mailem na adresu regulace@nukib.cz s předmětem „**Návrh nového ZKB – připomínka veřejnosti 2023**“, nejpozději do **12. března 2023 včetně**.

Datum:	9.3.2023	Navrhuje (jméno, příjmení, případně organizace):	Výbor nezávislého ICT průmyslu z. s.
Kontaktní údaje pro potřeby konzultace a zaslání vypořádání (e-mail, telefon):			Bc. Jakub Rejzek, MBA, LL.M., Tel: +420 727 938 968 Email: jakub.rejzek@vnictp.cz

Výbor nezávislého ICT průmyslu z. s. zastupuje celou řadu podnikatelů v ICT oborech. K připomínkám Výboru nezávislého ICT průmyslu z. s. se připojují také tyto firmy:

ABAK, spol. s r.o., AIRWAYNET a.s., Allstar Net s.r.o., Alternetivo s.r.o., Altnet s.r.o., AmigoNet s.r.o., Avonet s.r.o., BNET Bussines, s.r.o, ČD - Telematika a.s., Quantcom, a.s. (dříve Dial Telecom, a.s.) a jeho dceřiné společnosti zaměřené na retail, Discomp s.r.o., EDERA Group a.s., ELDATA pražská s.r.o., enovation s.r.o., Fastport a.s., FDLnet.CZ, s.r.o., FlowCutter s.r.o, GEMNET s. r. o., INTERNEXT 2000, s.r.o. , Optické sítě s.r.o., IXPERTA s.r.o., JaroNet - services s.r.o., JON.CZ s.r.o., LAYJET Czech Republic s. r. o., LBnet. cz s.r.o., Metropolnet a.s., MSC-NET s.r.o., MX-NET Telekomunikace s.r.o., 4NET.tv solution a.s.; Náš-Net Group s.r.o., Net-Connect s.r.o., SferiaNET.CZ s.r.o., SITEL, spol. s r.o., SMART Comp. a.s. (NEJ.TV), sledovanitv.cz s.r.o., Sys-DataCom s.r.o., Tlapnet s.r.o., Telly s.r.o., TKC system s.r.o., TNtech, s.r.o., Turbonet s.r.o., United Networks SE, UPC Česká republika, s.r.o., člen skupiny VODAFONE. VNICTP nezastupuje společnost Vodafone v záležitostech týkajících se mobilních sítí, ÚVT Internet s.r.o., Úvalská stavební s.r.o., Vlašimnet s.r.o., WIA spol. s r.o., Casablanca INT, s. r. o., VanCo.cz s.r.o., VIRIDIUM.CZ s.r.o., WMS s.r.o., za200.cz s.r.o. a neuvedení přidružení členové.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Např.: Zákon o kybernetické bezpečnosti, § X Vymezení pojmů	*Např.: Změnit v definici pojmu (…) slovo (…) na slovo (…)*	*Např.: Původně navrhovaná definice neuvádí důležitý znak tohoto pojmu, a to (…). Navrhovaná změna tento nedostatek odstraní.*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 8 Řízení aktiv, písmeno e).	Doplnit identifikaci a evidenci vazeb následujícím textem: e) identifikuje a eviduje relevantní vazby mezi aktivy ***a to způsobem, který odráží reálný stav v libovolném okamžiku***,	Původní definice nebere v úvahu změny v prostředí a vazby mezi aktivy. Změny v prostředí přináší značné riziko a znesnadňují šetření kybernetických bezpečnostních incidentů či reakce na vzniklé kybernetické bezpečnostní incidenty.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 11 Bezpečnost lidských zdrojů, odstavec 2), písmeno b) a c).	Doplnit mezi povinné role rozvoje bezpečnostního povědomí vývojáře: b) poučení uživatelů, administrátorů, ***vývojářů*** a osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice, c) potřebná teoretická i praktická školení uživatelů, administrátorů, ***vývojářů*** a osob zastávajících bezpečnostní role,	Do rozsahu rozvoje bezpečnostního povědomí je vhodné doplnit i vývojáře podílející se na vývoji informačních aktiv. Vývojáři představují značné riziko v případě, že postupy vývoje informačních systémů nebudou realizovány s ohledem na zásady bezpečného vývoje.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 28 Zabezpečení	Doplnit nový bod g): g) Povinná osoba vyhodnocuje kybernetické bezpečnostní události podle § 24 v prostředí průmyslových,	Schopnost vyhodnocovat kybernetické bezpečnostní události v prostředí průmyslových a řídících systémů patří k základu pro řízení kybernetických rizik v tomto prostředí.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
průmyslových, řídicích a obdobných specifických technických aktiv	řídících a obdobných specifických aktivech.		
Nejasnost kritérií velikosti	Ve vyhlášce o regulovaných službách v Příloze v bodě 16.1 a 16.2 sjednotit kritéria na 350 000 SIM karet nebo pevných přípojek. Alternativně obě tato kritéria zrušit a ponechat pouze dělení vyplývající ze směrnice	Na českém trhu je běžné, že řada operátorů provozuje své sítě jako holding menších společností. Jde o reziduum toho, že některé operátorské skupiny zvláště regionálních hráčů vznikly tak, že provedly akvizice menších hráčů. Protože operátoři mají různé využité technologie, různé dodavatele, různé topologie sítí a různou praxi v nasazování technologií do sítě, má smysl docházet k nějakému sjednocování až v určitém čase, případně - pokud tak operátorské holdingy seznají, že je to vhodné - k technologické unifikaci nedojít vůbec. Takto vzniklé skupiny mohou překonat NÚKIBem stanovený limit 100 tisíc aktivních pevných přípojek, ačkoli de facto jde o malé podniky. Vzhledem k této běžné praxi jsme přesvědčeni, že by NÚKIB měl ustoupit od stanovení objemových kritérií v oblasti pevných sítí, nebo je sjednotit se stanoveným limitem pro mobilní sítě (350 tisíc aktivních přípojek). I dle Výroční zprávy ČTÚ lze dovodit, že takto stanovené kritérium by přivedlo do množiny regulovaných dle Mechanismu	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		mnohé subjekty, na které NUKIB i dle vlastních vyjádření vůbec nemíří. Zároveň žádáme o upřesnění toho, jak bude NÚKIB postupovat v případě operátorů, kteří nabízí své služby formou tzv. Fixed Wireless Access (FWA) na kmitočtech, které jsou určené pro služby IMT (3400-3800 MHz). Tito operátoři nabízí službu, kterou pro některé regulatorní účely ČTÚ označuje jako pevnou službu, ale zároveň ji nabízí na zařízeních, které mohou mít v sobě SIM kartu a služba je nabízena na kmitočtech harmonizovaných pro pohyblivou službu. Potenciálně mohou mít tito operátoři časem více než 100 tisíc zákazníků.	
Bezpečnost dodavatelských řetězců Oddělení NIS 2 a BDŘ	Oddělit obě úpravy a projednávat je zvlášť, aby nebyla odložena včasná implementace směrnice.	Připadá nám nešťastné spojování mechanismu prověřování bezpečnosti dodavatelů a NIS 2. Mechanismus je dle NÚKIB národní úprava, která je neprojednaná a nejde o implementaci směrnice. Předpokládáme, že k této části nového zákona bude největší množství připomínek a tato problematika bude diskutovaná nejvíce, protože představuje největší zásah do svobody podnikání pro značnou část trhu.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zrušení vyhlášky o nepominutelných funkcích	Zrušit zmocnění vydat vyhlášku o nepominutelných funkcích a vyhlášku samotnou. Nebo Stanovit rozsah tak, aby postihoval část sítě, která je kritická (např. "páteřní síť" ze schématu NGN sítě nové generace, kterou používá v dotačních výzvách MPO - obr. 1 na straně 19 zde: https://www.mpo.cz/assets/cz/podnikani/dotace-a-podpora-podnikani/oppik-2014-2020/vyzvy-op-pik-2020/2020/3/Priloha-c--4_Pravidla-pro-zadatele-a-prijemce---Zvlastni-cast.pdf. Je zároveň nezbytné, aby rozsah nebyl stanoven vyhláškou, ale přímo zákonem.	NÚKIB v měsících předcházejících vydání tohoto návrhu vždy uváděl, že mechanismus prověřování bezpečnosti dodavatelských řetězců bude využívat principy vycházející z analýzy rizik, tedy uznání toho, že provozovatel zná své systémy a infrastrukturu nejlépe a je schopný zhodnotit riziko narušení bezpečnosti sám. V návrhu ale přistoupil k naprosto opačnému přístupu, kdy povinným osobám zároveň ukládá provést analýzu rizik (kdy poskytovatel má postupem podle vyhlášky ohodnotit dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká nebo kritická, ale zároveň sám stanovuje kritickou část stanoveného rozsahu jako aktiva stanoveného rozsahu, která zajišťují nepominutelné funkce stanoveného rozsahu podle vyhlášky. To je zcela v rozporu s principem analýzy rizik, protože stát direktivně stanovuje, na co mechanismus dopadne. V důvodové zprávě NÚKIB píše, že bez nepominutelných funkcí by byla "aktivace mechanismu posuzování dodavatelů odvislá pouze od subjektivního způsobu určení kritické části stanoveného rozsahu." To, zda daný provozovatel určil kritickou část stanoveného rozsahu správně, přitom může NÚKIB vymáhat v rámci kontrolní činnosti. Protože sítě operátorů jsou odlišné, využívají odlišnou topologii a provoz, může i identifikace	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		aktiv na úrovni vysoká nebo kritická být u různých operátorů různá, což je ale naprosto správné a odpovídá to principu řízení rizik na základě jejich analýzy. Nelze podceňovat také sílu mitigace rizik, která se může aplikace od aplikace výrazně lišit. Tento přístup významně upřednostňujeme, protože je v souladu s obecnými principy řízení kybernetické bezpečnosti. Ale pokud chce NÚKIB sám stanovovat povinný rozsah, nemá smysl zatěžovat povinné osoby identifikací aktiv, která mají být předmětem mechanismu. NÚKIB by si tak měl vybrat mezi oběma přístupy, ale nekombinovat je. Pokud už by si NÚKIB vybral přístup, kde vyjmenovává konkrétní funkcionality,	
Nejasná implementace článku 22 NIS 2	Nahradit mechanismus prověřování dodavatelů participací v koordinovaném posouzení dodavatelských řetězců, které předpokládá směrnice a které zjevně směřuje ke stejnému cíli s nižšími náklady. Pokud NÚKIB chce postupovat vlastní cestou, musí podrobně odůvodnit, proč je tato cesta vhodnější a odpovídá zásadě proporcionality. Do RIA doplnit reálné a konkrétní dopady na mikropodniky,	Zároveň kromě toho, že mechanismus je přijímán jako národní úprava nad rámec NIS 2 v rámci zajištění národní bezpečnosti, postrádáme pečlivé zdůvodnění, proč se stát nerozhodl jít v tomto případě implementací směrnice NIS 2, která předpokládá v článku 22 přesně to, čeho chce stát dosáhnout vlastním mechanismem – tedy posouzení bezpečnosti rizik dodavatelských řetězců u specifických kritických služeb ICT, systémů ICT nebo produktů ICT, a to se zohledněním technických, případně netechnických faktorů. V souladu se zásadou proporcionality by měl NÚKIB zdůvodnit, z jakého	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	malé a střední podniky a analýzu problému (tedy jací dodavatelé jsou přítomní v jaké části infrastruktury, která má podléhat mechanismu prověřování dodavatelského řetězce).	důvodu není toto ustanovení dostatečné a nevede k cíli, kterého chce stát dosáhnout, ale jiným a eurokonformnějším způsobem. Je zcela legitimní otázka, jakým způsobem článek 22 směrnice NÚKIB do zákona implementuje. Na schůzce s ICTU NÚKIB uvedl v prezentaci, že "Zmocnění dle čl. 22 NIS2 nesouvisí s vnitrostátním mechanismem, ale míří k podobnému cíli." Pak vůbec nerozumíme tomu, proč toto zmocnění NÚKIB k onomu cíli nevyužívá, ale jde vlastní cestou. Pokud mu to přikázala Bezpečnostní rada státu, je na místě příslušné usnesení BRS změnit dle aktuálního finálního znění směrnice (to ještě v době, kdy NÚKIB dostal od BRS úkol, nebylo k dispozici), které umožňuje lepší dosažení cíle, nebo podrobně a jasně odůvodnit v RIA, proč tak NÚKIB nepostupuje. Koordinované posouzení rizik dodavatelských řetězců na evropské úrovni odstraní mnoho nejasností, které jsou bohužel přítomné v současném návrhu. Protože dle článku 22 specifické služby, systémy a produkty ICT určí Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA, nedojde k závažnému narušení jednotného trhu, kdy dnes reálně hrozí, že operátoři v jedné zemi (a v jedné podnikatelské skupině) budou	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		moci využívat větší množství dodavatelů, než v zemi jiné. Tím se operátoři v zemi, kde stát úředně omezí množství dostupných dodavatelů, dostanou do konkurenční nevýhody, protože se jim logicky zvýší náklady – tím se stanou méně atraktivní pro potenciální investory a sníží se valuace jejich společností, což bude mít vliv na případný exit majitelů nebo na získání strategických investorů. NÚKIB by měl tyto aspekty zhodnotit podrobně v analýze RIA, kde zcela absentují. Stejně tak případné omezení dodavatelů významně ovlivní investiční kapacitu a schopnosti především menších a středních firem investovat do rozvoje svých sítí. Pokud budou NÚKIB nějací dodavatelé omezeni nebo zakázáni, pochopitelně to sníží úroveň konkurence a zvýší ceny. V praxi je běžné, že někteří dodavatelé vůbec s menšími podniky nekomunikují, případně jim nastavují ceníky bez možnosti smysluplné obchodní replikace. Jenom a pouze konkurenční prostředí na straně dodavatelů technologií zajišťuje schopnost inovací také pro MSP, a to až do úrovně opravdu velkých středních podniků, které nejsou zároveň mobilními operátory.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Navíc – jak argumentujeme níže – je velmi pravděpodobné, že mechanismus "zasáhne" operátory, na které nominálně nedopadá, protože ti jsou velkoobchodními partnery operátorů strategické infrastruktury, a protože rozsah strategicky významné infrastruktury je velmi široký a může zahrnovat takřka celou síť poskytovatele služeb elektronických komunikací. NÚKIB by měl zhodnotit vliv na malé a střední podniky v RIA. Není možné do RIA napsat (strana 15 a 16 v RIA), že "Vyčíslení nákladů není dobře možné, protože do něj vstupuje řada neznámých proměnných, a to zejména jak často bude nutné přistoupit k omezení některého z dodavatelů, v jakém rozsahu bude omezovaný dodavatel ve strategické infrastruktuře zastoupen a jaký způsob reakce na dané omezení přijme konkrétní povinná osoba mechanismu." Předpokládáme, že NÚKIB má k dispozici analýzu, kteří dodavatelé jsou zastoupeni v infrastruktuře, kterou míní mechanismem regulovat. RIA musí obsahovat kvalitní analýzu, jaký dopad bude reálně mechanismus mít na trh, tak jak to požadují např. poradní orgány vlády, konkrétně NERV.[1]	

[1] https://www.vlada.cz/assets/media-centrum/aktualne/Navrh-opatreni-.pdf

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Stanovení povinných osob mechanismu	V zákoně i prováděcích vyhláškách je nutné lépe specifikovat, kdo je dodavatel a jak konkrétně bude probíhat prověřování dodavatele a jak budou kritéria konkrétně uplatňována. V současné době ve vyhlášce o kritériích rizikovosti ani v zákoně není specifikovaný postup, jakým bude NÚKIB v prověřování postupovat, jakou váhu budou mít jednotlivá kritéria a jak bude NÚKIB postupovat v prověřování subdodavatelů. Postup nemůže být „blackbox“, musí jít o transparentní a zákonem daný přístup. Zároveň kritéria nesmí být ve vyhlášce, ale přímo v zákoně.	V telekomunikacích jsou naprosto běžné velkoobchodní vztahy mezi operátory, kteří si pronajímají navzájem či jeden druhému část infrastruktury, a to navíc různou formou (od pronájmu kapacity až po IRU). Koncept “dodavatele”, který NÚKIB představil v návrhu zákona, je zjevně postavený na představě regulátora, že povinná osoba si všechny služby zajišťuje sama prostřednictvím vlastní infrastruktury a tu staví na základě vztahů s dodavateli technologie. Tak to může být v řadě případů, ale v řadě případů ne. Zvlášť když NÚKIB ve vyhlášce “nepominutelné funkce” definuje tak, že jejich interpretace může být nejasná (např. bod 1.6 “Infrastrukturní služby nezbytné pro podporu provozu veřejné komunikační sítě a veřejné dostupné služby elektronických komunikací.”) či v bodě 1.1. část, která uvádí “ služby či komponenty významné co do velikosti zeměpisné oblasti pokrytí nebo počtu připojených uživatelů”, což může být fakticky cokoli). Je tak nejasné, jak bude přistupovat např. povinný subjekt mechanismu ke svým dodavatelům datových okruhů, kteří mají sídlo v ČR a jsou tak subjektem českého, potažmo evropského práva, ale zároveň nejsou	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		subjekty mechanismu, takže nepodléhají prověřování rizik spojených s dodavatelem. Zároveň není jasné, jak k takovým subjektům bude přistupovat při prověřování NÚKIB. V §X Řízení dodavatelů a vztah k zadávání veřejných zakázek je sice uvedeno, že "Poskytovatel regulované služby je povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro svůj stanovený rozsah a tyto požadavky zanést do smlouvy, kterou s dodavatelem uzavře." ale je zcela nejasné, jak to má být provedené v realitě, kdy poskytovatel nějaké služby může mít dodávanou službu zajišťovanou pomocí konglomerátru subjektů, kteří mohou mít různé dodavatele, subdodavatele a sub-subdodavatele různých IT řešení a systémů a dodávat ji koncovému zákaznkovi jako funkční celek na základě SLA. V § X Prověřování rizik spojených s dodavatelem, odstavci 3 c) se mluví o "poddodavatelích". Vyplývá z toho, že prověřování budou zřejmě čelit i menší subjekty a pokud ano, do jakého "kolene"? Typicky je např. běžné, že operátor s regionálně rozsáhlou optickou sítí, který má např. 40 tisíc aktivních pevných přípojek, je dodavatelem služeb okruhu, VO konektivity či jiných služeb na různých úrovních vrstvy	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		OSI pro operátory s celostátní působností nebo operátorům, kteří mají větší množství aktivních pevných přípojek. Dopadne na tyto společnosti mechanismus prověřování dodavatele skrz jejich potenciální dodávky větším subjektům, nebo nikoli?	
Nejasná kritéria toho, kdo je "dodavatel"	Lépe specifikovat, kdo je dodavatel, subdodavatel a jaký vliv to bude mít na posuzování NÚKIB.	V § X Prověřování rizik spojených s dodavatelem, odstavci 3 c) se hovoří o tom, že "dodavatelem bezpečnostně významné dodávky každý, kdo povinné osobě mechanismu prověřování poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku." Protože pravomoci NÚKIB v prověřování jsou velmi rozsáhlé, je potřeba jasně definovat konkrétně, jak bude k jednotlivým dodavatelům NÚKIB přistupovat a kdo jsou "poddodavatelé". Ve vyhlášce o kritériích rizikovosti dodavatele totiž není vůbec jasné, jakou váhu jednotlivým kritériím bude úřad dávat nebo jakým způsobem je bude vyhodnocovat (§ 4 vyhlášky dává úřadu v tomto naprosto volnou ruku). Základní zdůvodnění existence mechanismu (a ve vyhlášce o kritériích rizikovosti dodavatele je to v §2 výslovně zmíněné) je přesvědčení NÚKIB, že na dodavatele mohou mít "vliv" nedemokratické země a	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		některé země jim mohou přikazovat např. spolupráci se zpravodajskými službami a podobně. NÚKIB argumentuje tím, že takoví dodavatelé mohou mít ve svých systémech záměrné zranitelnosti (viz strany 7 a 8 RIA k BDŘ). V zákoně ani vyhláškách jsme ale nenalezli jasnou definici toho, kdo je tím "dodavatelem". Řada výrobců telekomunikačních technologií má v zemích, které mohou být vyhodnocené jako rizikové, výzkum, vývoj nebo výrobu, případně velkou část svého dodavatelského řetězce. Někteří si nechávají svoje technologie vyvinout a vyrobit na zakázku od OEM a ODM výrobců. Není nám jasné, jak máme přistupovat k těmto dodavatelům - budou označení jako riziková, protože mají část dodavatelského řetězce v nedemokratických zemích, nebo nebudou riziková, protože mají sídlo v zemi EU nebo NATO? NÚKIB v RIA argumentuje (strana 7) tím, že "Hardwarová a softwarová řešení informačních a komunikačních technologií jsou již natolik komplexní a v infrastrukturách povinných osob mechanismu tak četně zastoupená, že je nelze technicky komplexně včas a efektivně prověřovat." Platí to pouze pro infrastrukturu	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		povinných osob mechanismu, nebo i pro dodavatele samotné? Část výrobců má totiž velmi rozsáhlý dodavatelský řetězec, aby dokázali splnit požadavky zákazníků. Své produkty skládají dohromady díky designu, výzkumu, vývoji a výrobě v různých zemích světa, z nichž určitá část zřejmě může být NÚKIB hodnocena jako země, které mohou mít na dodavatele vliv. Velcí dodavatelé mají např v Číně velká výzkumná a vývojová centra formou dceřiných společností (či joint ventures), které bezpochyby splňují obavy NÚKIB vyjádřené na str. 8 mechanismu, tedy že mají buňku KS Číny, která má dosah na dění ve společnosti. Zároveň často není jasné, kdo je oním výrobcem, zvláště to platí u komoditizovaných technologií, které jsou nasazované v transportní vrstvě či přístupové vrstvě sítě. V jedné dodávce určené pro ČR od jednoho "výrobce" (tedy značky) je možné nalézt výrobky vyrobené v Číně, Indii nebo Malajsii. Konečný dodavatel (ten, který produkt navrhl a prodává jej pod svou značkou) řeší samozřejmě testování a bezpečnost	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		pomocí svých vlastních interních procesů, které má certifikované, ale otázkou je, zda to bude stačit pro prověřování strategické bezpečnosti, které chce NÚKIB provádět. Typicky nás zajímají následující scénáře a přístup NÚKIB k nim: • Koncový dodavatel z demokratické země, vývoj a výzkum v nedemokratické zemi, výroba v nedemokratické zemi • Koncový dodavatel z demokratické země, vývoj a výzkum v nedemokratické zemi, výroba v demokratické zemi • Koncový dodavatel z demokratické země, vývoj a výzkum v demokratické zemi, výroba v nedemokratické zemi	
Praktické fungování mechanismu	NÚKIB by měl nahradit OOP jiným vhodnějším instrumentem	V § X Omezení rizik spojených s dodavatelem popisuje úřad, že vydá "opatření obecné povahy, ve kterém povinným osobám mechanismu prověřování stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		stanoveného rozsahu, zjistí-li možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku v důsledku vyhodnocení kritérií rizikovosti dodavatele." Zároveň úřad píše v odstavci 2, že vyzve "všechny povinné osoby mechanismu prověřování a dodavatele bezpečnostně relevantní dodávky, vůči jehož plnění opatření obecné povahy míří, aby k návrhu opatření obecné povahy podávali ve lhůtě 30 dnů připomínky." Znamená to že pokud jeden operátor identifikuje určité prvky v síti jako klíčové z hlediska bezpečnosti, mají všechny ostatní povinné osoby mechanismu právo se vyjádřit k OOP a úřad jejich připomínky vypořádá (ekvivalent veřejné konzultace podle § 130 ZEK u OOP vydávaných ČTÚ). Kromě nevhodnosti využití institutu OOP k tomuto účelu (nedostatečná ochrana práv zúčastněných subjektů) vnímáme další problémy. Sítě každého poskytovatele jsou navržené každá jinak a mohou mít každá jiné kritické systémy. Pokud jeden operátor uvede, že určitá část sítě je "kritickou částí stanoveného rozsahu", a NÚKIB bude prověřovat dodavatele, bude vydané OOP	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		platné pro konkrétní část sítě a funkcionalitu daného operátora, nebo bude mít obecnou platnost pro všechny poskytovatele služeb elektronických komunikací, kteří mohou mít sítě navržené jiným způsobem? Jak bude NÚKIB postupovat, pokud někteří operátoři budou některé části sítě považovat za kritické a jiné ne? Bude se zákaz vztahovat na dodavatele a konkrétní zařízení v konkrétním použití? Zároveň vnímáme i bezpečnostní problém OOP, pokud správně rozumíme tomu, jak jej chce NÚKIB využívat. Na semináři CZ.NIC NÚKIB prezentoval, že OOP se bude vždy vztahovat na konkrétní kritickou část stanoveného rozsahu příslušné povinné osoby v režimu vyšších povinností, ale k dispozici bude před vydáním ke konzultaci všem dotčeným osobám (což chápeme, protože takový je smysl OOP), tedy adresátem budou všechny povinné osoby mechanismu stanovené vyhláškou o regulovaných službách a dodavatelé technologie. Toto může mít dvojí důsledek - buď bude odůvodnění OOP extenzivní a pak bude podrobně identifikovat kritickou část sítě v dokumentu přístupném široké veřejnosti, což znamená významné bezpečnostní riziko (poskytovatelé obvykle nemají	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zájem na tom, aby široká veřejnost věděla potenciálně citlivé informace o jejich systémech) nebo bude identifikace systému, na který OOP dopadá významně omezena (podobně jako v OOP identifikujících KII, které vydává úřad podle stávajícího ZKB) a pak bude fakticky nemožné se k němu nějak smysluplně vyjádřit pro dodavatele nebo pro další povinné osoby. Obojí je špatně, a mimo jiné i proto OOP není vhodný instrument k tomu účelu.	
Problematika DNS	Upravit znění vyhlášky tak, aby reflektovala dopad jen na otevřené veřejné poskytovatele služeb DNS, tedy odstranit odkaz na poskytovatele veřejně dostupné služby elektronických komunikací nebo zajištění veřejně dostupné sítě elektronických komunikací a ujasnit, že zákon nedopadá na DNS, které poskytují operátoři v rámci své sítě svým zákazníkům.	Dle Vyhlášky o regulovaných službách je v bodě 16.4 zahrnutý do regulovaných subjektů i Poskytovatel služeb DNS. Směrnice uvádí v článku 3 odst 1b), že za základní subjekty (v novém ZKB poskytovatelé služeb v režimu vyšších povinností) se považují "kvalifikovaní poskytovatelé služeb vytvářejících důvěru, registry domén nejvyšší úrovně a provozovatelé DNS bez ohledu na jejich velikost. Vyhláška pak poskytovatele služeb DNS specifikuje takto: "Poskytovatel služeb DNS, s výjimkou operátorů kořenových jmenných serverů, je poskytovatel	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		regulované služby v režimu vyšších povinností v případě, že a) aktivně poskytuje veřejně dostupné rekurzivní služby pro překlad jmen domén (rekurzivní DNS) koncovým uživatelům internetu, a zároveň poskytuje veřejně dostupnou službu elektronických komunikací nebo zajišťuje veřejnou komunikační síť elektronických komunikací podle zákona o elektronických komunikacích, b) poskytuje autoritativní služby pro překlad jmen domén (autoritativní DNS) pro použití třetí stranou, a zároveň správu nebo hosting více než 10 000 domén druhého řádu.” Pokud NÚKIB implementuje směrnici tímto způsobem, tak do bodu “a)” spadnou desítky malých a mikropodniků - poskytovatelů služeb elektronických komunikací, kteří by jinak byli v režimu nižších povinností dle bodu 16.1 či 16.2. Celá řada operátorů totiž poskytuje svým zákazníkům služby DNS, protože to pro ně představuje součást zajištění kvalitního poskytování služby přístupu k internetu, pomáhá to pro vyšší zajištění kybernetické bezpečnosti (je možné snáze	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		blokovat malware a phishing domény) a je to pro ně praktické z důvodu plnění jiných povinností (např. povinnosti blokování stránek s nelegální nabídkou léčivých přípravků nebo nelegálním hazardem) Domníváme se, že NÚKIB zde nesprávně implementuje směrnici zbytečně tvrdým způsobem. Ve směrnici je uvedeno v recitálu 32, že "by se měla vztahovat na registry domén nejvyšší úrovně a provozovatele systému překladu jmen domén (dále jen „provozovatel DNS") považované za subjekty poskytující veřejně dostupné rekurzívní služby pro překlad jmen domén pro koncové uživatele internetu." DNS poskytované operátory ale nejsou veřejné - pro libovolné uživatele internetu - ale jsou využitelné pouze pro zákazníky daného operátora. To, že operátor je poskytovatel "veřejně dostupné služby elektronických komunikací" v tomto nehraje roli, "veřejnost" oné služby spočívá v tom, že z jejího využívání není nikdo předem vyloučen. Naopak "veřejně dostupné" DNS servery jsou k dispozici pro každého uživatele internetu, jde například o služby jako OpenDNS společnosti CISCO, 1.1.1.1 od společnosti Cloudflare, Google Public DNS, Quad9 a podobně. Jsme přesvědčeni - i na základě popisu postupu institucí	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		během schvalování směrnice, který NÚKIB popsal v důvodové zprávě - že úmysl zákonodárce byl postihnout tyto služby a nikoli vlastní DNS operátorů. Pokud bude NÚKIB na výkladu v návrhu trvat, výsledkem bude, že regionální operátoři - aby se vyhnuli takřka automatickému přesunu do vyšších povinností - budou místo vlastních DNS serverů využívat služeb managed DNS, což jim zvýší náklady a paradoxně to může zvýšit riziko dostupnosti služeb, protože v případě nedostupnosti poskytovatele managed DNS služby bude zasaženo více koncových uživatelů, než pokud si DNS zajišťují malí operátoři sami.	
Poskytování služby sítě pro doručování obsahu (CDN)	Apelujeme na NÚKIB, aby významně omezil uvalené regulační povinnosti dle článku 21 pro služby sítě pro doručování obsahu do doby, než komise přijme prováděcí akty, které předpokládá článek 21 odstavec 5. Vzhledem k tomu, že směrnice předpokládá přijetí těchto prováděcích aktů, je velmi pravděpodobné, že úmyslem	NÚKIB nijak nedefinuje, co je to síť pro doručování obsahu (CDN). Úřad v důvodové zprávě uvádí, že "v otázce přesné transpozice požadavku směrnice nemohl oslovit žádného konkrétního gestora, jelikož tito poskytovatelé nejsou definováni odkazem na jiný právní předpis a nespadají do působnosti jednoho konkrétního regulátora či gestora. Síť pro doručování obsahu podle čl. 6 bodu 32 směrnice je síť geograficky distribuovaných serverů za účelem zajištění vysoké dostupnosti, přístupnosti nebo rychlého poskytování digitálního	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zákonodárce bylo nevystavovat tento typ regulovaných subjektů stejným povinnostem (nebo stejně vymáhaným povinnostem) jako zbylé subjekty, protože vnímá jejich specifičnost a odlišnost. Toto vnímání ale v návrzích vyhlášek chybí.	obsahu a služeb uživatelům internetu jménem poskytovatelů obsahu a služeb. Na základě těchto informací návrh vyhlášky definuje službu jako poskytování služby sítě pro doručování obsahu (CDN). Dle našeho názoru míří směrnice na poskytovatele CDN typu Akamai, Amazon CloudFront, Azure CDN, Netflix Open Connect a podobně, což je vidět např. z recitálu 113, kde se mluví o "přeshraniční povaze služeb" mimo jiné i poskytovatelů sítí pro doručování obsahu. Za "poskytovatele služeb sítě pro doručování obsahu" ale mohou být označeny i menší české platformy pro šíření IPTV - v závislosti na výkladu NÚKIB - které ale mohou plnit kritéria středního podniku. Směrnice a její implementace tak vytváří regulatorní bariéru vstupu na trh pro menší české firmy, které už tak mají obtíže konkurovat velkým poskytovatelům IPTV, kteří kromě úspor z rozsahu disponují i televizními právy na atraktivní obsah a podobně. Je otázka, zda skutečně zákonodárce zamýšlel, aby směrnice dopadla i na tento typ podnikatelů, kteří se zabývají pouze maximálně efektivní distribucí videoobsahu pro své partnerské sítě (především menší lokální a regionální operátory).	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 4	Nepominutelné funkce stanoveného rozsahu by neměly být stanoveny vyhláškou, kterou vydává NÚKIB	Není vhodné, aby stanovení tzv. nepominutelných funkcí, jak je předpokládá návrh nového ZKB a vyhláška o nepominutelných funkcích, bylo svěřeno výlučně do rukou jednoho orgánu (NÚKIB), jemuž by tímto bylo v zásadě ponecháno volné uvážení o tom, jakých aktiv a procesů se bude týkat tzv. mechanismus posuzování bezpečnosti dodavatelského řetězce, a též v zásadě volná dispozice měnit, co je za nepominutelnou funkci považováno. Tato předpokládaná pravomoc soustředěná v NÚKIB je nevhodná zejména v kontextu celkového rozsahu pravomocí, které návrh nového zákona o kybernetické bezpečnosti svěřuje NÚKIBu. NÚKIB by totiž měl ve svém souhrnu určovat nejen rozsah mechanismu (na které nepominutelné/kritické funkce se má vztahovat), ale také které osoby mají podléhat povinnostem dle mechanismu, jakož i kritéria rizikovosti dodavatelů. NÚKIB sám pak má prověřovat rizika spojená s dodavatelem, přičemž i sám rozhodne, které subjekty osloví pro poskytnutí informací pro hodnocení dodavatelů (a koho ne) a vyhodnotí kritérií rizikovosti dodavatelů na základě vlastního uvážení a následně má	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		mít oprávnění vydat opatření obecné povahy (OOP), proti němuž není přípustný opravný prostředek. Celý proces prověření, hodnocení a případného omezení či zakázání dodavatele je tak od počátku čistě ve výlučné režii NÚKIB a dotčené subjekty se k němu v zásadě ani nemohou vyjádřit (nejde o klasické správní řízení).	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 4 Vyhláška o regulovaných službách, § 6 Kritéria pro určení poskytovatele regulované služby, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce	NÚKIB nemá mít oprávnění určit rozhodnutím, že poskytovatel regulované služby v režimu vyšších povinností má plnit povinnosti mechanismu prověřování bezpečnosti dodavatelského řetězce a ukládat mu povinnost plnit povinnosti dle mechanismu	Je nevhodné, aby do pravomoci NÚKIB spadala možnost na základě vlastního uvážení jednostranně určovat, které subjekty se stanou povinnými osobami dle mechanismu a budou povinny plnit povinnosti v návaznosti na mechanismus stanovené. Takové rozhodování hrozí arbitrárností a není v souladu se zásadou právní jistoty. Tato předpokládaná pravomoc NÚKIB je nevhodná zejména v kontextu celkového rozsahu pravomocí, které návrh nového zákona o kybernetické bezpečnosti svěřuje NÚKIBu. NÚKIB by totiž měl ve svém souhrnu určovat nejen kritéria rizikovosti dodavatelů, ale také rozsah mechanismu (na které nepominutelné/kritické funkce se má vztahovat), a rovněž které osoby mají podléhat povinnostem dle mechanismu. NÚKIB sám pak má prověřovat rizika spojená s dodavatelem, přičemž i	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		sám rozhodne, které subjekty osloví pro poskytnutí informací pro hodnocení dodavatelů (a koho ne) a vyhodnotí kritérií rizikovosti dodavatelů na základě vlastního uvážení a následně má mít oprávnění vydat opatření obecné povahy (OOP), proti němuž není přípustný opravný prostředek. Celý proces prověření, hodnocení a případného omezení či zakázání dodavatele je tak od počátku čistě ve výlučné režii NÚKIB a dotčené subjekty se k němu v zásadě ani nemohou vyjádřit (nejde o klasické správní řízení)	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem	Případné prověřování bezpečnosti dodavatelského řetězce má probíhat ve vztahu ke konkrétní bezpečnostně-relevantní dodávce a z hlediska konkrétních rizik a zranitelností s ní spojených	NÚKIB prvotně deklaroval, že mechanismus bude postaven na základě principů analýzy rizik. Nyní však na toto své tvrzení rozporoval na semináři Hospodářské komory konaném dne 24. 2. 2023, kde uvedl, že v rámci prověřování bude posuzována pouze osoba dodavatele, a to bez kontextu konkrétní bezpečnostně-relevantní dodávky. NÚKIB tedy nebude posuzovat konkrétní rizika a zranitelnosti spojené s konkrétní dodávkou. V rámci prověřování tak nebudou hodnocena a zohledňována ani již zavedená bezpečností opatření povinných osob.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Tomuto přístupu odpovídá i nová forma rozhodování, kdy NÚKIB v návrhu nového zákona o kybernetické bezpečnosti zvolil formu opatření obecné povahy (OOP), které pro konkrétně vymezený předmět (tj. zde stanovení podmínek/omezení nebo zákaz využití plnění dodavatele) zavazuje obecně vymezený okruh adresátů (zde povinných osob mechanismu prověřování), tedy případné omezení nebo zákaz využití plnění dodavatele se vztáhne na všechny povinné osoby mechanismu. Bez ohledu na to, jaká bezpečnostní opatření (např. diverzifikace dodavatelů jako postup doporučený EU Toolboxem) již dotčené povinné osoby zavedly. Takový postup vnímáme nejen jako excesivní zásah do svobody podnikání, ale i potenciál k ohrožení celého segmentu MSP. NUKIB nedohlédne na vliv takového rozhodnutí na podnikatele, kteří nemají přístup k omezeným dodávkám od některých dodavatelů, jejich případným výrobním výpadkům či nedostatku kapacity vytvářet obchodní vztahy s menšími podniky v ICT. Na příkladu společnosti Samsung můžeme ukázat příklad. Dodávky 5G řešení od této společnosti pro MSP byly odmítnuty kvůli nedostačené kapacitě implementačního týmu; společnost se věnuje pouze celostátním podnikům. Dalším, tentokrát bezpečnostním argumentem, je	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nutnost diverzifikovat dodavatele jako základní opatření proti výpadkům dodávek či náhrady technologií při případném kyberbezpečnostním problému, viz. úmyslný backdoor v amerických zařízeních Ubiquity a CISCO.	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem a § X Omezení rizik spojených s dodavatelem	Prověřování dodavatele a přijímání opatření dle § X Omezení rizik spojených s dodavatelem by nemělo výt ve výlučné dikci NÚKIB; prověřování dodavatele by měla provádět komise složená ze zástupců ministerstev, orgánů veřejné správy a zástupců dotčených subjektů	Dle našeho názoru by proces prověřování rizik spojených s dodavatelem a navazujících opatření (OOP) neměl být prováděn výlučně NÚKIB, ale mělo by se jednat o výsledek kolektivního rozhodování více zúčastněných subjektů. Jako vhodné kompromisní a proporcionální řešení se jeví uplatnění rakouského modelu – tedy vytvoření komise složené ze zástupců ministerstev, orgánů veřejné správy, ale i zástupců dotčených subjektů, kteří přijímají usnesení jako společný výbor/komise. Podobný poradní sbor je i ve Finsku, které NÚKIB uvádí jako jednu z inspirací pro svůj návrh. V českém prostředí by tato komise přijímající rozhodnutí v procesu prověřování dodavatelů měla být tvořena ČTÚ a zástupci dalších regulatorních úřadů v dotčených oblastech (mj. energetika, doprava a další), MPO a zástupci příslušných dotčených osob.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem a § X Omezení rizik spojených s dodavatelem	Poskytovatelé regulované služby by měli mít možnost předkládat komisi návrhy a materiály k posouzení	Dotčené regulované subjekty (poskytovatelé regulovaných služeb) a dodavatelé by měli mít možnost předkládat výboru/komisi, jejíž zřízení bylo navrženo v předchozí námitce, návrhy a materiály k posouzení, tak jak je tomu např. u záruky dle německého modelu.	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem a § X Omezení rizik spojených s dodavatelem	Výsledky prověřování dodavatelů a vydání omezujících opatření by mělo být projednáno v komisi a schváleno nadpoloviční většinou hlasů členů komise	Výsledky prověřování bezpečnosti dodavatelského řetězce a dodavatelů, jakož i případná navazující omezující opatření by měla být důkladně projednána v rámci komise, přičemž by jejich vydání bylo podmíněno jejich schválením většinou hlasů členů komise.	
Zákon o kybernetické bezpečnosti, § X Omezení rizik spojených s dodavatelem	Nadbytečnost, neproporcionalita a nepřiměřená tvrdost ustanovení o vydání opatření obecné povahy (OOP) – ustanovení by mělo být vypuštěno	Dle § X Varování odst. 1 (s.14 návrhu zákona) vydá NÚKIB varování, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti. Vzhledem k nově navržené úpravě, kdy dle § X Varování odst. 2 (s.14 návrhu zákona) platí, že poskytovatel regulované služby v režimu vyšších povinností je povinen provádět povinnosti stanovené varováním (varování je pro tyto poskytovatele závazné, nemá již jen formu doporučující), se zavedení institutu OOP jeví jako účelové a nadbytečné, neboť je zřejmé, že stejného výsledku v oblasti kybernetické bezpečnosti lze	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dosáhnout i na základě nově upraveného znění institutu varování. Nepřiměřená tvrdost OOP je podtržena též skutečností, že proti OOP (a tedy jí stanovených omezení či zákazů obchodních vztahů s určitými dodavateli) není možné bránit se opravným prostředkem (proti OOP nelze podat odvolání ani rozklad), což dále přispívá k netransparentnosti celého procesu a možné arbitrárnosti rozhodování NÚKIB). Možnost vydávání opatření obecné povahy v rámci mechanismu by tedy měla být odstraněna.	
Zákon o kybernetické bezpečnosti, § X Omezení rizik spojených s dodavatelem	Stanovení přiměřené lhůty pro plnění povinnosti stanovené opatřením obecné povahy (OOP)	Za předpokladu, že by v novém zákoně o kybernetické bezpečnosti zůstalo ponecháno ustanovení o OOP, navrhujeme, aby v obecně závazném opatření (OOP) byla přímo uvedena přiměřená lhůta, od kdy má být příslušné bezpečnostní opatření přijato nebo od kdy se povinná osoba omezí nebo se zdrží užívání dodávek daného dodavatele, přičemž tato lhůta nesmí být ze zákona kratší než 10 let (s ohledem na zásadu respektování životního cyklu technologií).	
Zákon o kybernetické bezpečnosti, Mechanismus prověřování	Nutnost zajištění respektování životního cyklu technologií	Ve zveřejněné zprávě RIA k návrhu zákona o kybernetické bezpečnosti je deklarováno, že: *„V případě*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
bezpečnosti dodavatelského řetězce (obecně), § X Omezení rizik spojených s dodavatelem		*zákazu dodavatele bude stanovena přechodná lhůta, do jejíž uplynutí musejí povinné osoby tento zákaz reflektovat, která bude reflektovat životní cyklus dodávaných technologií a bude v řádech několika let*.“ V samotném návrhu zákona o kybernetické bezpečnosti však tato zásada není reflektována a jsme toho názoru, že je nutné ji v připravované legislativě výslovně zakotvit. Tato lhůta by měla být minimálně 10 let (viz výše).	
Zákon o kybernetické bezpečnosti, § X Omezení rizik spojených s dodavatelem	Podmínění vydání opatření obecné povahy (OOP) neodstraněním zjištěného rizika ze strany povinné osoby mechanismu prověřování	Jakákoli omezující opatření by mělo být možné uložit pouze v případě, že příslušné povinné osoby mechanismu prověřování neodstranily rizika zjištěná v souladu s mechanismem prověřování.	
Vyhláška o nepominutelných funkcích stanoveného rozsahu, Příloha, bod 1 - Nepominutelné funkce ve veřejné komunikační síti	Nepominutelné funkce ve veřejné síti dle bodu 1.15 by neměly být řazeny mezi nepominutelné funkce stanoveného rozsahu	Jsme toho názoru, že nepominutelné funkce stanovené v bodu 1.15 přílohy, tj: - 1.15: Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic; by neměly být řazeny k nepominutelným funkcím, neboť k ním vzhledem ke své povaze a z ní vyplývající nižší závažnosti a důležitosti potenciálních rizik, nenáleží.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o nepominutelných funkcích stanoveného rozsahu, Příloha, bod 1 - Nepominutelné funkce ve veřejné komunikační síti	Potřeba splnění základních kritérií stanovených v bodu 1.1 Přílohy vyhlášky i pro body 1.2 až 1.16 Přílohy vyhlášky	Bod 1.1 Přílohy vyhlášky o nepominutelných funkcích stanoveného rozsahu obsahuje poměrně obecný popis nepominutelných funkcí včetně řízení sítových zdrojů a jiné kontroly nebo řízení provozu koncových uživatelů ve veřejné komunikační síti a jiného řízení nebo řízení provozu koncových uživatelů, přičemž je posuzován i dopad jeho narušení na síťový provoz a význam tohoto dopadu. Další funkce uvedené v Příloze vyhlášky pod body 1.2 až 1.16 na rozdíl od bodu 1.1. uvádí výčet specifických funkcí, u nichž není výslovně dáno, že by měly splňovat i kritéria obecného rázu stanovená v bodu 1.1 Přílohy vyhlášky. Navrhovatel je toho názoru, že by obecná kritéria, která jsou uvedena v bodu 1.1 vyhlášky měla být s ohledem na zásadu proporcionality vztažena a uvedena i pro další specifické nepominutelné funkce ve veřejné komunikační síti uvedené v bodech 1.2 až 1.16 Přílohy vyhlášky.	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 3	Provádění (sebe)hodnocení aktiv dle odst. 3 § X Prověřování rizik spojených s dodavatelem, by mělo být prováděno pouze v případech, kdy	Je-li stanoven seznam kritických (nepominutelných) funkcí pro určitý sektor, pak by povinným osobám mechanismu prověřování mělo stačit pouze	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o nepominutelných funkcích stanoveného rozsahu Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností	není prováděcím předpisem stanoven seznam kritických (nepominutelných) funkcí	identifikovat kritické části podle daného seznamu a není nutné další vlastní (sebe)hodnocení aktiv, které předpokládá odst. 3 § X Prověřování rizik spojených s dodavatelem. Pokud pro daný sektor není stanoven seznam kritických (nepominutelných) funkcí, pak je na místě sebehodnocení pro stanovení kritických funkcí. Před zveřejněním nového seznamu kritických (nepominutelných) funkcí je vždy třeba konzultovat dotčené sektory. Stát by měl vytvořit (jak navrhujeme výše) poradní sbor složený mimo jiné i ze zástupců nominovaných průmyslem (nominujícími subjekty mohou být subjekty zastoupené v Radě hospodářské a sociální dohody a/nebo povinné subjekty pro připomínkové řízení), který by funkce, na které dopadá mechanismus, projednával a byl by odborným partnerem státu.	
Zákon o kybernetické bezpečnosti, § X Podmínky lokalizace informací a dat Vyhláška o bezpečnostních opatřeních pro poskytovatele	Vypuštění ustanovení § X Podmínky lokalizace informací a dat ze zákona o kybernetické bezpečnosti a ustanovení § 29 vyhlášky Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností	Navržená úprava zásadním způsobem přesahuje rámec implementace směrnice NIS2 a rozsah požadovaných povinností kladený na povinné subjekty je zcela neodůvodněný. Navrhovatel je tedy názoru, že by dané ustanovení zákona a vyhlášky mělo být vypuštěno.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu vyšších povinností, § 29			
Zákon o kybernetické bezpečnosti, § X Opatření k řešení stavu kybernetického nebezpečí	Opatření uvedená v odst. 1 písm. c), e) a h) § X Opatření k řešení stavu kybernetického nebezpečí mohou být využita pouze v případě nouzového stavu vyhlášeného vládou	Opatření uvedená v odst. 1 písm. c), e) a h) § X Opatření k řešení stavu kybernetického nebezpečí, tj: - nařízení práce v pohotovostním režimu, - zákaz orgánům a osobám, které k tomu byly NÚKIB vyzvány, používání technických aktiv v případě, že jsou taková aktiva bezprostředně ohrožena kybernetickým bezpečnostním incidentem, který je může významně poškodit nebo zničit, nebo jsou takovým incidentem již postižena, - nařízení orgánům a osobám zpřístupnění neveřejných komunikačních sítí v jejich správě pro potřeby NÚKIB, jsou natolik závažná, že jejich zavedení by mělo být podmíněno vyhlášením nouzového stavu vládou, nikoli jen vyhlášením stavu kybernetického nebezpečí, jenž vyhlašuje ředitel NÚKIB.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem; Vyhláška o kritériích rizikovosti dodavatele	Je nutná změna celkového přístupu k posuzování rizikovosti dodavatele – rizikovost dodavatele by měla být posuzována zejména na základě technických kritérií, nikoli vágních strategických kritérií	Kritéria pro posuzování dodavatele by měla být technická, mimo jiné včetně kvality produktů dodavatele a postupů kybernetické bezpečnosti. Hodnocení by mělo založeno na objektivních technických kritériích a reflektovat, zda dodavatel získal nějaký certifikát kybernetické bezpečnosti; zda může dodavatel poskytnout prohlášení/dohodu o kybernetické bezpečnosti/ochraně údajů; zda ze strany dodavatele někdy došlo k porušení jakéhokoli požadavku nebo povinnosti týkající se kybernetické bezpečnosti nebo ochrany údajů; zda nedošlo k nějakým kybernetickým bezpečnostním incidentům souvisejícím s produkty dodavatele v důsledku selhání dodavatele; analýzu rizik produktů dodavatele; zda jsou aktuálně zavedená zmírňující opatření a procesy a postupy v pořádku.	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem; Vyhláška o kritériích rizikovosti dodavatele	Rizikovost dodavatele by měla být posuzována zejména na základě technických kritérií, nikoli na základě země původu	Kritérium země původu by nemělo být rozhodné při posuzování rizikovosti dodavatele. Hodnocení by mělo probíhat na základě technických kritérií, včetně posuzování technických zranitelností a též specifických rizik podle zásad řízení aktiv a rizik.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, Mechanismus prověřování bezpečnosti dodavatelského řetězce	Nutnost zabránit kumulaci pravomocí v rukách jen jednoho úřadu a preferovat spíše rozhodování kolektivní (v komisi složené z více subjektů)	NÚKIB by se v návaznosti na předkládanou legislativu stal úřadem, který by měl mít kontrolu nad dodavatelským řetězcem kritických odvětví, která by on sám současně definoval a mohl jejich rozsah modifikovat dle svého uvážení (zejm. vyhláškami). Pokud by byla přijata právní úprava v předložené podobě, NÚKIB by přebíral kompetence vlády, když by ve své podstatě mohl určoval zahraniční politiku České republiky a zasahovat i do oblasti národní bezpečnosti. Úkolem NÚKIB je provádění činností v oblasti kybernetické bezpečnosti, v zákonem vymezených mantinelech, a v rámci regulované infrastruktury řízení regulovaných subjektů a nápomoc zvyšovat kybernetickou odolnost těchto subjektů. Určování zahraniční politiky (byť nepřímo) do jeho kompetencí nenáleží. Tímto postupem by NÚKIB mohl zhoršit jak mezinárodní, tak hospodářské postavení České republiky. Spatřujeme také riziko v možnosti přímo ovlivňovat zátěž pro jednotlivé tržní segmenty, jakožto důsledků takových rozhodnutí není schopen NUKIB dohlédnout. Nikoliv ve smyslu aktuálního hrozby, ale v budoucnu by mohla taková moc v rukou	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nekolektivního orgánu vytvářet extrémní korupční riziko.	
Zákon o kybernetické bezpečnosti, Mechanismus prověřování bezpečnosti dodavatelského řetězce	Nutnost konkretizace a transparentnosti právní úpravy	Rozhodování NÚKIB o potenciální rizikovosti dodavatelů je dle navržené úpravy do značné míry netransparentní. Problémem je v tomto směru zejména jednostranný, takřka nenapadnutelný, způsob určování regulovaných odvětví, netransparentní hodnocení významu kritérií rizikovosti dodavatelů a zemí, utajování informací, z nichž se při rozhodování vychází, jakož i parametrů jejich hodnocení. Je nutné předmětné aspekty a kritéria konkretizovat a doplnit příslušnými metodikami. Je třeba také vyloučit korupční riziko.	
Zákon o kybernetické bezpečnosti, Mechanismus prověřování bezpečnosti dodavatelského řetězce	Nutnost reflektovat veškeré dopady navrhované právní úpravy a významně doplnit RIA	Je zapotřebí, aby v rámci připravované právní úpravy byly reflektovány veškeré relevantní dopady, což v případě nového zákona o kybernetické bezpečnosti, a zejména jeho části týkající se mechanismu, není splněno, a to zejména pokud jde o možné finanční a hospodářské dopady navrhované právní úpravy. Navrhovaná právní úprava by měla být nastavena tak, aby co nejméně zatěžovala povinné subjekty, nikoli jim hrozila finančními ztrátami v některých případech až do výše miliard a tento potenciální dopad současně zcela ignorovala. Je třeba významným způsobem doplnit RIA	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		o tyto aspekty, tak aby odpovídala požadavkům na kvalitu, které doporučuje NERV (viz výše). Jsme toho názoru, že návrh RIA si dokonce v několika bodech protiřečí. V případě Důvodové zprávy máme obavu, že by mohlo dojít k paušalizování jednotlivých pochybení neřízení se Doporučením na celý trh. Kyberbezpečnostní opatření v ICT a telco oborech bere drtivá většina podnikatelů velmi vážně.	
Zákon o kybernetické bezpečnosti, Mechanismus prověřování bezpečnosti dodavatelského řetězce	Potřeba nenarušování legitimního očekávání subjektů a podnikatelského prostředí	Předkládané legislativní návrhy v současné podobě narušují legitimní očekávání povinných osob, neboť zcela zásadní aspekty mechanismu (včetně rozsahu regulace a povinných subjektů) mohou být ze strany NÚKIB v zásadě snadno jednostranně měněny (vzhledem k tomu, že NÚKIB přijímá vyhlášky tyto oblasti blíže upravující) a rovněž může dojít k zákazu či významnému omezení jejich dodavatelů. Takto rozsáhlá rozhodovací pravomoc poskytuje velký prostor pro libovůli při rozhodování NÚKIB a představuje tak rozsáhlé riziko. Proto by měla být navržená podoba mechanismu a otázka jeho zavedení přehodnocena. Nepřiměřeně přísná úprava tak může vést nejen k úplnému dlouhodobému zastrašení podnikatelských	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		subjektů od spolupráce s dodavateli z vybraných zemí, což ohrožuje prosperitu České republiky, rozvoj její ICT infrastruktury a schopnost práce s ve světě jinak běžnými technologiemi na projektech v zahraničí.	

Jakub Rejzek

Digitally signed by Jakub Rejzek
Date: 2023.03.10 11:42:21 +01'00'