Zámer národného projektu Operačného programu Integrovaná infraštruktúra Prioritná os 7 Informačná spoločnosť

Názov národného projektu: Vybudovanie nosnej infraštruktúry bezpečného informačno-komunikačného systému FS SR

1. Zdôvodnite čo najpodrobnejšie prečo nemôže byť projekt realizovaný prostredníctvom výzvy na predkladanie žiadostí o NFP?
   (napr. porovnanie s realizáciou prostredníctvom dopytovo orientovaného projektu vzhľadom na efektívnejší spôsob napĺňania cieľov OP, efektívnejšie a hospodárnejšie využitie finančných prostriedkov)

Navrhovaný projekt „Vybudovanie nosnej infraštruktúry bezpečného informačno-komunikačného systému FS SR“ súvisí so zvýšením úrovne kybernetickej bezpečnosti informačno-komunikačného prostredia Finančnej správy Slovenskej republiky (ďalej len „FS SR“), vybudovaním nosnej infraštruktúry FS SR na monitoring, analýzu a aktívnu ochranu pred kybernetickými hrozbami, ako aj informačného systému na bezpečnú a monitorovanú manipuláciu s citlivými a utajovanými informáciami v elektronickej podobe. Riešenie pre zvýšenie úrovne kybernetickej bezpečnosti je koncipované ako komplexný mechanizmus, ktorý chráni FS SR pred vonkajšími ako aj vnútornými rizikami a hrozbami. Tento mechanizmus môže byť účinný len v prípade, že jeho jednotlivé časti a komponenty budú navzájom previazané a budú úzko spolupracovať. Zvýšenie úrovne kybernetickej bezpečnosti pomocou tohto riešenia sa predpokladá najmä v oblasti:

- ochrany perimetra, bezpečnostného monitoringu a analytiky,
- digitalizácie, šifrovania a riadenia prístupu v rámci tvorby, uchovávania a výmeny citlivých informácií a utajovaných skutočností.

Požiadavkou projektu je v zmysle schválenej Národnej koncepcie informatizácie verejnej správy Slovenskej republiky (ďalej aj „NKIVS“) – časť Bezpečnostná architektúra a Zákona o KyB nadviazať na nosné bloky bezpečnostnej architektúry a tieto stavebné prvky v prostredí FS SR maximálne využiť.
Štúdia, vychádzajúc z vyhodnotenia možností dosiahnutia požadovaného nového cieľového stavu, sa zameriava predovšetkým na posúdenie možností implementácie nového bezpečnostného informačného systému, ktorý bude prostredníctvom nových elektronických služieb slúžiť na podporu plnenia úloh a činnosti FS definovaných zákonom, ktoré spadajú do jej pôsobnosti.
Navrhované riešenie nadväzuje a vychádza najmä z nasledujúcich strategických dokumentov:

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES.
- Operačný program Integrovaná infraštruktúra 2014 – 2020, Prioritná os číslo 7 Informatizácia spoločnosti.
- Národná koncepcia informatizácie verejnej správy Slovenskej republiky.
- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020.
- Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020.
- Dohovor Rady Európy o predchádzaní terorizmu.

- Medzinárodný dohovor o potláčaní financovania terorizmu.
- Európsky dohovor o potláčaní terorizmu.
- Dohovor OSN proti nadnárodnému organizovanému zločinu.
- Dohovor vypracovaný na základe článku K.3 Zmluvy o Európskej únii o vzájomnej pomoci a spolupráci medzi colnými správami (oznámenie č. 245/2009 Z. z.).
- Rozhodnutie Rady 2009/917/SVV z 30. novembra 2009 o využívaní informačných technológií na colné účely (Ú. v. EÚ, L323, 10.12.2009).
- Akčný plán EÚ na posilnenie boja proti daňovým podvodom a daňovým únikom, KOM(2012) 722, Brusel, 6.12.2012.
- Akčný plán boja proti daňovým podvodom na roky 2012 až 2016, schválený uznesením Vlády SR č. 235 z 31.5.2012, Akčný plán boja proti daňovým podvodom na roky 2017 až 2018, schválený uznesením Vlády SR č. 206 z 26.4.2017, Akčný plán boja proti daňovým podvodom na roky 2018 až 2020.
- Národná stratégia ochrany finančných záujmov EÚ v SR, schválená uznesením Vlády SR č. 18 zo 7.1.2015.
- Návrh smernice Európskeho parlamentu a Rady o predchádzaní využívania finančného systému na účely prania špinavých peňazí a financovania terorizmu, KOM(2013) 45, Brusel, 5.2.2013.
- Návrh riadenia Európskeho parlamentu a Rady o údajoch, ktoré sprevádzajú prevody finančných prostriedkov, KOM (2013) 44, Brusel, 5.2.2013.
- Akčný plán EÚ pre boj proti terorizmu, 2011.
- Národný akčný plán boja proti terorizmu schválený uznesením Vlády SR č. 316 z 18.5.2011.
- Národný akčný plán boja proti terorizmu na roky 2015 – 2018 schválený uznesením Vlády SR č. 213/2015 z 29.4.2015.

Prijímateľom národného projektu bude Finančné riaditeľstvo SR.
FS SR plní úlohy podľa zákona č. 333/2011 Z. z. v rozsahu svojej pôsobnosti a aj ďalšie úlohy podľa osobitných zákonov a úloh vyplývajúcich taktiež z medzinárodných zmlúv a dohôd o spolupráci s orgánmi a medzinárodnými organizáciami a inštitúciami v rámci spolupráce členských štátov EÚ, ktorými je SR viazaná.

2. Príslušnosť národného projektu k relevantnej časti operačného programu

Prioritná os	7 Informačná spoločnosť
Investičná priorita	Posilnenie aplikácií IKT v rámci elektronickej štátnej správy, elektronického vzdelávania, elektronickej inklúzie, elektronickej kultúry a elektronického zdravotníctva.
Špecifický cieľ	7.9: Zvýšenie kybernetickej bezpečnosti v spoločnosti
Miesto realizácie projektu (na úrovni kraja)	Banskobystrický kraj Bratislavský kraj Nitriansky kraj Košický kraj Prešovský kraj Trenčiansky kraj Trnavský kraj Žilinský kraj
Identifikácia hlavných cieľových skupín (ak relevantné)	Inštitúcie a subjekty verejnej správy

3. Prijímateľ[1] národného projektu je **Finančné riaditeľstvo SR**

Dôvod určenia prijímateľa národného projektu[2]	FS SR plní úlohy podľa zákona č. 333/2011 Z. z. v rozsahu svojej pôsobnosti a aj ďalšie úlohy podľa osobitných zákonov a úloh vyplývajúcich taktiež z medzinárodných zmlúv a dohôd o spolupráci s orgánmi a medzinárodnými organizáciami a inštitúciami v rámci spolupráce členských štátov EÚ, ktorými je SR viazaná.
Má prijímateľ osobitné, jedinečné kompetencie na implementáciu aktivít národného projektu priamo zo zákona, osobitných právnych predpisov, resp. je uvedený priamo v príslušnom operačnom programe?	Áno, viď. vyššie.
Obchodné meno/názov (aj názov sekcie ak relevantné)	Finančné riaditeľstvo SR
Sídlo	Lazovná ulica č. 63, 974 01 Banská Bystrica
IČO	42499500

4. Partner, ktorý sa bude zúčastňovať realizácie národného projektu (ak relevantné)

Zdôvodnenie potreby partnera národného projektu (ak relevantné)[3]	N/A
Kritériá pre výber partnera [4]	
Má partner monopolné postavenie na implementáciu týchto aktivít? (áno/nie) Ak áno, na akom základe?	
Obchodné meno/názov	
Sídlo	
IČO	

V prípade viacerých partnerov, doplňte údaje za každého partnera.

5. Predpokladaný časový rámec

Dátumy v tabuľke nižšie nie sú záväzné, ale predstavujú vhodný a žiadúci časový rámec pre zabezpečenie procesov, vedúcich k realizácii národného projektu.

Dátum vyhlásenia vyzvania vo formáte Mesiac/Rok	04/2019
Uveďte plánovaný štvrťrok podpísania zmluvy o NFP s prijímateľom	4 Q/2019

[1] V tomto dokumente je používaný pojem prijímateľ a žiadateľ. Je to tá istá osoba, no technicky sa žiadateľ stáva prijímateľom až po podpísaní zmluvy o NFP.

[2] Jednoznačne a stručne zdôvodnite výber prijímateľa NP ako jedinečnej osoby oprávnenej na realizáciu NP (napr. odkaz na platné predpisy, operačný program, národnú stratégiu, ktorá odôvodňuje jedinečnosť prijímateľa NP).

[3] Uveďte dôvody pre výber partnerov (ekonomickí, sociálni, profesijní...). Odôvodnite dôvody vylúčenia akejkoľvek tretej strany ako potenciálneho realizátora.

[4] Uveďte, na základe akých kritérií bol partner vybraný, alebo ak boli zverejnené, uveďte odkaz na internetovú stránku, kde sú dostupné. Ako kritérium pre výber - určenie partnera môže byť tiež uvedená predchádzajúca spolupráca žiadateľa s partnerom, ktorá bude náležite opísaná a odôvodnená, avšak nejde o spoluprácu, ktorá by v prípade verejných prostriedkov spadala pod pôsobnosť zákona o VO.

Uveďte plánovaný štvrťrok spustenia realizácie projektu	1 Q/2020
Predpokladaná doba realizácie projektu v mesiacoch	24 mesiacov

6. Finančný rámec

Alokácia na vyzvanie (zdroj EÚ a ŠR)	43 374 580,88 EUR
Celkové oprávnené výdavky projektu	43 374 580,88 EUR
Vlastné zdroje prijímateľa	N/A

7. Východiskový stav
   a. Uveďte východiskové dokumenty na regionálnej, národnej a európskej úrovni, ktoré priamo súvisia s realizáciou NP:
      - Zákon č. 333/2011 Z. z. o orgánoch štátnej správy v oblasti daní, poplatkov a colníctva v znení neskorších predpisov.
      - Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES.
      - Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.
      - Zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o eGovernmente), v znení neskorších predpisov.
      - Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
      - Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
      - Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.
      - Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
      - Rozhodnutie Rady EU 2013/488/EU z 23.9.2013 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ.
      - Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.
      - Zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
      - Výnos Ministerstva financií SR č. 55/2014 o štandardoch pre informačné systémy verejnej správy, a výnos č. 137/2015 Z. z. ktorým sa mení a dopĺňa predošlý výnos č. 55/2014.,
      - Vyhláška NBÚ č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
      - Vyhláška NBÚ č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
      - Vyhláška NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,

- Vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
- Vyhláška NBÚ č. 48/2019 Z.z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností.

b. Uveďte predchádzajúce výstupy z dostupných analýz, na ktoré nadväzuje navrhovaný zámer NP (štatistiky, analýzy, štúdie,...):
   - Hlavný dokument štúdie uskutočniteľnosti: (dostupný na https://wiki.vicepremier.gov.sk/display/SU/SU-MD-su_342),
   - CBA rozpočet: (dostupný na: https://metais.vicepremier.gov.sk/studia/detail/e5b7aad4-f99d-317b-a248-6f3f81a10a21?tab=documents)

c. Uveďte, na ktoré z ukončených a prebiehajúcich národných projektov[5] zámer NP priamo nadväzuje, v čom je navrhovaný NP od nich odlišný a ako sú v ňom zohľadnené výsledky/dopady predchádzajúcich NP (ak relevantné):

   Zámer NP priamo nenadväzuje na žiadny z ukončených ani prebiehajúcich národných projektov.

d. Popíšte problémové a prioritné oblasti, ktoré rieši zámer národného projektu. (Zoznam známych problémov, ktoré vyplývajú zo súčasného stavu a je potrebné ich riešiť):
   - Problém: Na základe interných analýz a posudzovaní stavu bezpečnosti IS FS SR možno konštatovať, že aktuálny stav obsahuje značné množstvo zraniteľností, ktoré je potrebné adresovať, aby nedošlo k ich zneužitiu.
   - Problém: Súčasný bezpečnostný systém funguje na zastaranej architektúre a nepokrýva všetky informačné aktíva FS SR. V rámci svojej infraštruktúry eviduje FS SR 99 informačných systémov, z toho vyše 20 dôležitých.
   - Problém: Infraštruktúra v súčasnosti obsahuje izolované prvky bezpečnostnej architektúry, ktoré primárne fungujú len na vybraných zariadeniach a systémoch, teda nie sú nasadené plošne.
   - Problém: Aktuálny systém zabezpečenia a ochrany nespĺňa všetky požiadavky legislatívy (najmä zákona o KyB). Pokuta za nedodržanie legislatívnych požiadaviek zákona o utajovaných skutočnostiach je 10 miliónov EUR, v prípade incidentu z dôvodu nedodržania požiadaviek 20 miliónov EUR.
   - Problém: Systém nie je prispôsobený na súčasné bezpečnostné požiadavky, čoho dôsledkom je, že nemusia byť identifikované všetky bezpečnostné incidenty. Priemerná výška ekonomických dopadov jedného incidentu je 103 045,09 EUR.
   - Problém: Výmena citlivých informácií a utajovaných skutočností je aktuálne založená na manuálnom prenose v rámci pracovísk FS dislokovaných v celej SR. Počet písomností za rok, ktoré sa distribuujú manuálne, je 3418 a zamestnanci najazdia počas ich prenosu 1,2 milióna kilometrov.

[5] V prípade ak je to relevantné, uveďte aj ukončené národné projekty z programového obdobia 2007-2013.

e. Popíšte administratívnu, finančnú a prevádzkovú kapacitu žiadateľa a partnera (v prípade, že v projekte je zapojený aj partner)

Žiadateľ

Administratívna kapacita interná – Požiadavky interných administratívnych rolí budú plnené internými zdrojmi.

Administratívna kapacita externá – Dodávateľsky sa plánujú zabezpečiť vybrané podporné aktivity.

Finančná kapacita – Obstarávacie prostriedky a prevádzkové náklady počas trvania projektu budú financované z fondov EÚ, po skončení projektu bude prevádzka riešenia financovaná zo štátneho rozpočtu.

Prevádzková kapacita – predpokladá sa zabezpečenie prevádzky riešenia internými pracovníkmi.

8. Vysvetlite hlavné ciele NP (stručne):
   (očakávaný prínos k plneniu strategických dokumentov, k socio-ekonomickému rozvoju oblasti pokrytej OP, k dosiahnutiu cieľov a výsledkov príslušnej prioritnej osi/špecifického cieľa)

Účelom projektu je podporiť program digitalizácie a elektronizácie služieb verejnej správy SR s cieľom zefektívniť procesy činnosti FS SR, nadviazať na aktivity realizované v súčasnom období v oblasti zavádzania eGovernmentu v SR, nadviazať na strategické a koncepčné dokumenty v oblasti digitalizácie a elektronizácie služieb verejnej správy schválené Vládou SR, ako aj na aktivity v rámci EÚ, ktoré sú v tejto oblasti realizované a to pri zabezpečení vysokej miery kybernetickej bezpečnosti.

Cieľom projektu je:

- Zabezpečenie súladu s požiadavkami legislatívy, najmä zákona o KyB.
- Implementovanie moderných a efektívnych nástrojov a technológií pre kybernetickú ochranu a monitorovanie bezpečnostných incidentov (aj v reálnom čase) a poskytnutie efektívnych nástrojov a prostriedkov pre riadenie prípadných bezpečnostných incidentov a obnovu prevádzkovaných systémov FS SR.
- Implementovanie nástrojov identifikácie a analýz hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky a nástrojov zabezpečujúcich ochranu sieťového perimetra FS SR s prepojením na centrálny monitorovací systém.
- Riadenie a správa agendy súvisiacej s vytváraním, výmenou a manipuláciou s citlivými a utajovanými skutočnosťami v oblastiach vymedzených pre FS SR zákonom, jej modernizácia a odbúranie jej papierovej podoby s prepojením na centrálny monitorovací systém.

Takto koncipovaný projekt zabezpečí:

- efektívnejšiu prácu útvarov FS SR (znížením administratívneho zaťaženia a skrátením času potrebného na vykonávanie úkonov spojených s administratívnou bezpečnosťou pri manipulácii s citlivými a klasifikovanými informáciami),
- vysokú kvalitu práce a pracovného prostredia pracovníkov (možnosť práce s citlivými a klasifikovanými informáciami od pracovného stola, možnosť využitia jednej pracovnej stanice na manipuláciu s informáciami rôzneho stupňa bezpečnostnej klasifikácie),

- vyššiu úroveň informačnej a kybernetickej bezpečnosti v rámci procesov monitoringu a riadenia bezpečnostných incidentov a riadenia vonkajších aj vnútorných hrozieb.

Potreba realizácie projektu vyplýva z postupnej informatizácie spoločnosti a jednotlivých orgánov štátnej správy, s ktorými FS SR spolupracuje v rozsahu potrebnom na plnenie úloh ustanovených zákonom, z nevyhnutnosti prispôsobiť informačné systémy FS SR potrebám, úrovni a požiadavkám systémov partnerských inštitúcií v rámci SR, ale aj v rámci členských krajín EÚ a nevyhnutnosti zefektívniť a skvalitniť prácu a výstupy činnosti FS SR.

9. Očakávaný stav a merateľné ciele

V tejto časti popíšte očakávané výsledky projektu s konkrétnym prínosom vo vzťahu k rozvoju oblasti pokrytej operačným programom a zrealizovaniu aktivít. V tabuľke nižšie uveďte projektové ukazovatele a iné údaje. Projektové ukazovatele musia byť definované tak, aby odrážali výstupy/výsledky projektu a predstavovali kvantifikáciu toho, čo sa realizáciou aktivít za požadované výdavky dosiahne.[6]				
Cieľ národného projektu	Merateľný ukazovateľ	Indikatívna cieľová hodnota	Aktivita projektu	Súvisiaci programový ukazovateľ[7]
Vytvorenie siete pokrývajúcej kybernetickú ochranu, perimetrovú ochranu IKT prostredia a sietí, analytiku a bezpečnostný monitoring stavu IB a KyB v informačnom prostredí FS SR, najmä implementáciou nástroja SIEM a implementáciou pokročilých, moderných a automatizovaných nástrojov na identifikáciu a analýzu hrozieb a anomálií v rámci sieťových tokov a	P0048 Dodatočný počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov.	1	Analýza a dizajn, Nákup HW a krabicového softvéru, Implementácia, Testovanie, Nasadenie	N/A

[6] V odôvodnených prípadoch sa uvedená tabuľka nevypĺňa, pričom je nevyhnutné do tejto časti uviesť podrobné a jasné zdôvodnenie, prečo nie je možné uviesť požadované údaje.
[7] Národný projekt by mal obsahovať minimálne jeden relevantný projektový ukazovateľ, ktorý sa agreguje do programového ukazovateľa. Pri ostatných projektových ukazovateľoch sa uvedie N/A.

sieťovej prevádzky, ako aj nástrojov zabezpečujúcich ochranu perimetra na úrovni databáz, webových portálov a domén s prepojením na centrálny systém SIEM.				

Iné údaje, ktorými je možné sledovať napĺňanie cieľov národného projektu (ak relevantné)				
Cieľ národného projektu	Ukazovateľ	Indikatívna cieľová hodnota	Aktivita projektu	

V prípade viacerých merateľných ukazovateľov, doplňte údaje za každý merateľný ukazovateľ.

10. Bližší popis merateľných ukazovateľov.[8]

Predmetná časť sa týka projektových ukazovateľov	
Názov merateľného ukazovateľa[9]	Dodatočný počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov.
Akým spôsobom sa budú získavať dáta?	Dáta pre overenie dosiahnutia merateľného ukazovateľa sa budú získavať overením skutočného stavu implementovaných nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov v rámci FS SR.

V prípade viacerých merateľných ukazovateľov, doplňte údaje za každý z nich.

11. Očakávané dopady

Zoznam prínosov a prípadných iných dopadov, ktoré sa dajú očakávať pre jednotlivé cieľové skupiny		
Dopady	Cieľová skupina (ak relevantné)	Počet[10]
Zvýšenie kybernetickej bezpečnosti, zefektívnenie výkonu a zníženie nákladov na fungovanie verejnej správy	Inštitúcie a subjekty verejnej správy	60%
Zabránenie škodám v prípade preventívne odhalených incidentov	Inštitúcie a subjekty	60%

[8] V odôvodnených prípadoch sa uvedená tabuľka nevypĺňa, pričom je nevyhnutné do tejto časti uviesť podrobné a jasné zdôvodnenie, prečo nie je možné uviesť požadované údaje.

[9] V prípade viacerých merateľných ukazovateľov, doplňte tabuľku za každý merateľný ukazovateľ.

[10] Ak nie je možné uviesť početnosť cieľovej skupiny, uveďte do tejto časti zdôvodnenie.

	verejnej správy	
Zabránenie škodám z incidentov, ktoré už nastali	Inštitúcie a subjekty verejnej správy	20%
Zníženie únikov informácií	Inštitúcie a subjekty verejnej správy	Vo výške 16 mil. EUR ročne (výpočet v zmysle CBA)
Prínosy z nahradenia transportu informácii elektronickou výmenou dát a z toho vyplývajúceho ušetrenia času, pohonných hmôt a amortizácie áut	Inštitúcie a subjekty verejnej správy	Vo výške 0,7 mil. EUR ročne (výpočet v zmysle CBA)

V prípade viacerých cieľových skupín, doplňte dopady na každú z nich.

12. Aktivity
a) Uveďte detailnejší popis aktivít.

V zmysle platnej Príručky pre žiadateľa pôjde o nasledujúce skupiny aktivít:

Hlavné aktivity:
- Nákup HW a krabicového softvéru

Podporné aktivity:
- Riadenie projektu

b) V tabuľke nižšie uveďte rámcový popis aktivít, ktoré budú v rámci identifikovaného národného projektu realizované a ich prepojenie so špecifickými cieľmi.

Názov aktivity	Cieľ, ktorý má byť aktivitou dosiahnutý (podľa sekcie *Očakávaný stav*)	Spôsob realizácie (žiadateľ a/alebo partner)	Predpokladaný počet mesiacov realizácie aktivity
Analýza a dizajn	Vytvorenie siete pokrývajúcej kybernetickú ochranu, perimetrovú ochranu IKT prostredia a sietí, analytiku a bezpečnostný monitoring stavu IB a KyB v informačnom prostredí FS SR,	Žiadateľ	12

	najmä implementáciou nástroja SIEM a implementáciou pokročilých, moderných a automatizovaných nástrojov na identifikáciu a analýzu hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky, ako aj nástrojov zabezpečujúcich ochranu perimetra na úrovni databáz, webových portálov a domén s prepojením na centrálny systém SIEM.		
Nákup HW a krabicového softvéru	Vytvorenie siete pokrývajúcej kybernetickú ochranu, perimetrovú ochranu IKT prostredia a sietí, analytiku a bezpečnostný monitoring stavu IB a KyB v informačnom prostredí FS SR, najmä implementáciou nástroja SIEM a implementáciou pokročilých, moderných a automatizovaných nástrojov na identifikáciu a analýzu hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky, ako aj nástrojov zabezpečujúcich	Žiadateľ	1

	ochranu perimetra na úrovni databáz, webových portálov a domén s prepojením na centrálny systém SIEM.		
Implementácia	Vytvorenie siete pokrývajúcej kybernetickú ochranu, perimetrovú ochranu IKT prostredia a sietí, analytiku a bezpečnostný monitoring stavu IB a KyB v informačnom prostredí FS SR, najmä implementáciou nástroja SIEM a implementáciou pokročilých, moderných a automatizovaných nástrojov na identifikáciu a analýzu hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky, ako aj nástrojov zabezpečujúcich ochranu perimetra na úrovni databáz, webových portálov a domén s prepojením na centrálny systém SIEM.	Žiadateľ	18
Testovanie	Vytvorenie siete pokrývajúcej kybernetickú ochranu, perimetrovú ochranu IKT prostredia a sietí, analytiku a	Žiadateľ	18

	bezpečnostný monitoring stavu IB a KyB v informačnom prostredí FS SR, najmä implementáciou nástroja SIEM a implementáciou pokročilých, moderných a automatizovaných nástrojov na identifikáciu a analýzu hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky, ako aj nástrojov zabezpečujúcich ochranu perimetra na úrovni databáz, webových portálov a domén s prepojením na centrálny systém SIEM.		
Nasadenie	Vytvorenie siete pokrývajúcej kybernetickú ochranu, perimetrovú ochranu IKT prostredia a sietí, analytiku a bezpečnostný monitoring stavu IB a KyB v informačnom prostredí FS SR, najmä implementáciou nástroja SIEM a implementáciou pokročilých, moderných a automatizovaných nástrojov na identifikáciu a analýzu hrozieb a	Žiadateľ	6

	anomálií v rámci sieťových tokov a sieťovej prevádzky, ako aj nástrojov zabezpečujúcich ochranu perimetra na úrovni databáz, webových portálov a domén s prepojením na centrálny systém SIEM.		
Podporné aktivity (Riadenie projektu)	Vytvorenie siete pokrývajúcej kybernetickú ochranu, perimetrovú ochranu IKT prostredia a sietí, analytiku a bezpečnostný monitoring stavu IB a KyB v informačnom prostredí FS SR, najmä implementáciou nástroja SIEM a implementáciou pokročilých, moderných a automatizovaných nástrojov na identifikáciu a analýzu hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky, ako aj nástrojov zabezpečujúcich ochranu perimetra na úrovni databáz, webových portálov a domén s prepojením na centrálny systém SIEM.	Žiadateľ	24

V prípade viacerých aktivít, doplňte informácie za každú z nich.

13. Rozpočet

Jasne uveďte, ako bol pripravovaný indikatívny rozpočet a ako spĺňa kritérium „hodnota za peniaze“, t. j. akým spôsobom bola odhadnutá cena za každú položku, napr. prieskum trhu, analýza minulých výdavkov spojených s podobnými aktivitami, nezávislý znalecký posudok, v prípade, ak príprave projektu predchádza vypracovanie štúdie uskutočniteľnosti, ktorej výsledkom je, o. i. aj určenie výšky alokácie, je potrebné uviesť túto štúdiu ako zdroj určenia výšky finančných prostriedkov. Skupiny výdavkov doplňte v súlade s MP CKO č. 4 k číselníku oprávnených výdavkov v platnom znení. V prípade operačných programov implementujúcich infraštruktúrne projekty, ako aj projekty súvisiace s obnovou mobilných prostriedkov, sa do ukončenia verejného obstarávania uvádzajú položky rozpočtu len do úrovne aktivít.

Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu a ich výstižné zdôvodnenie		
Predpokladané finančné prostriedky na hlavné aktivity	**Celková suma**	**Uveďte plánované vecné vymedzenie**
Analýza a dizajn	2 086 560 EUR	
Nákup HW a krabicového softvéru	31 616 565 EUR	Okrem nákupu HW a SW vybavenia, suma zahŕňa aj obstaranie licencií, licenčný poplatok na obdobie trvania a odborné školenia.
Implementácia	4 021 920 EUR	
Testovanie	1 965 600 EUR	
Nasadenie	2 328 480 EUR	
Hlavné aktivity SPOLU	**42 019 125 EUR**	
Predpokladané finančné prostriedky na podporné aktivity	**Celková suma**	**Uveďte plánované vecné vymedzenie**
Podporné aktivity (Riadenie projektu)	1 355 456 EUR	Suma za Riadenie projektu predstavuje 3% z celkových nákladov projektu.
Podporné aktivity SPOLU	**1 355 456 EUR**	
CELKOM	**43 374 581 EUR**	

14. Deklarujte, že NP vyhovuje **zásade doplnkovosti** (t. j. nenahrádza verejné alebo ekvivalentné štrukturálne výdavky členského štátu v súlade s článkom 95 všeobecného nariadenia).

Príspevok z EŠIF v tomto projekte nebude mať za následok zníženie vnútroštátnych štrukturálnych výdavkov a bude doplnkom vnútroštátneho verejného financovania v zmysle zásady doplnkovosti.

15. Bude v národnom projekte využité zjednodušené vykazovanie výdavkov? Ak áno, aký typ?

Nie.

16. Štúdia uskutočniteľnosti vrátane analýzy nákladov a prínosov
Informácie sa vypĺňajú iba pre investičné[11] typy projektov.

Štúdia uskutočniteľnosti vrátane analýzy nákladov a prínosov	
Existuje relevantná štúdia uskutočniteľnosti[12] ? (áno/nie)	áno
Ak je štúdia uskutočniteľnosti dostupná na internete , uveďte jej názov a internetovú adresu, kde je štúdia zverejnená	Hlavný dokument štúdie uskutočniteľnosti: (https://wiki.vicepremier.gov.sk/display/SU/SU-MD-su_342) CBA rozpočet: (https://metais.vicepremier.gov.sk/studia/detail/e5b7aad4-f99d-317b-a248-6f3f81a10a21?tab=documents)
V prípade, že štúdia uskutočniteľnosti nie je dostupná na internete, uveďte webové sídlo a termín, v ktorom predpokladáte jej zverejnenie (mesiac/rok)	N/A

[11] Investičný projekt – dlhodobá alokácia finančného aj nefinančného kapitálu na naplnenie investičného zámeru až do etapy, kedy projekt vstúpi do prevádzkovej etapy a prípadne začne generovať stabilné príjmy. Investičný projekt smeruje k: výstavbe stavby alebo jej technickému zhodnoteniu; nákupu pozemkov, budov, objektov alebo ich častí; nákupu strojov, prístrojov, tovarov a zariadení; obstaraniu nehmotného majetku vrátane softvéru. Zdroj: Uznesenie Vlády SR č. 300 z 21.6.2017 k návrhu Rámca na hodnotenie verejných investičných projektov v SR.
[12] Pozri aj Uznesenie Vlády SR č. 300 z 21.6.2017 k návrhu k návrhu Rámca na hodnotenie verejných investičných projektov v SR (dostupné na: http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=26598)