CALL: DIGITAL SECURITY FOCUS AREA
https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ds-2016-2017.html#c,topics=callIdentifier/t/H2020-DS-2016-2017/1/1/1&callStatus/t/Forthcoming/1/1/0&callStatus/t/Open/1/1/0&callStatus/t/Closed/1/1/0&+identifier/desc

DS-02-2016: Cyber Security for SMEs, local public administration and Individuals (IA – dot. 70%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Zameranie projektov na nasledujúce skupiny konečných užívateľov: malé a stredné podniky, miestna samospráva, jednotlivci (občania).
  Pri identifikovaní najrozšírenejších hrozieb a oblastí kyber bezpečnosti, ktorým čelia konečný užívatelia, žiadosti by mali vziať do úvahy sprievodné dokumenty, najlepšie postupy a štandardy vydané Medzinárodnou štandardnou organizáciou, technickým fórom a orgánmi členských štátov, ktoré sú prispôsobené malým a stredným podnikom alebo jednotlivcom. Žiadosti by mali aktívne prispieť rozvoju alebo zlepšeniu týchto dokumentov, postupov a štandardov.
  Žiadosti by mali obsahovať vytvorenie inovatívnych riešení s vysokým stupňom použiteľnosti a automatizácie pri zachovaní dostatočnej miery situačného prehľadu a kontroly v kyber priestore. Žiadosti by mali vziať do úvahy psychologické a behaviorálne faktory (vrátane rodovej otázky), ktoré ovplyvňujú kyber bezpečnosť na úrovni jednotlivca alebo organizácie. Žiadosti by mali overiť svoje návrhy prostredníctvom rozsiahlej spätnej väzby od užívateľov, prípadne zastúpením užívateľov v konzorciu, ak je to vhodné.

DS-04-2016: Economics of Cybersecurity (RIA – dot. 100%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Projekty by mali prijať prístup kombinujúci ekonomický, behaviorálny, spoločenský a technický náhľad, prístupy k meraniu a metodológie a kombinovanie metód z oblasti mikroekonomiky, econometriky, kvalitatívnych spoločenských vied, behaviorálnych vied, teórie rozhodovania, riadenia rizík a experimentálnej ekonomiky. Žiadosti by mali pokrývať jednu z nasledujúcich dvoch oblastí:
  - Kybernetický nákladovo-efektívny rámec:
    - Nákladové modely bezpečnosti a súkromia, vrátane oceňovania digitálnych aktív, modelovania a metód odhadu nákladov nehmotných rizík (reputácia, nekritické narušenie služby a pod.) a príslušných ukazovateľov
    - žiadosti by mali skúmať a zohľadniť príslušné osobitosti jednotlivých sektorov trhu, overiť modely relevantnými aktérmi z týchto sektorov
    - optimálne investície do bezpečnosti informácií, riadenia rizík a poistenia kybernetickej bezpečnosti
  - Stimuly a obchodné modely:
    - Identifikovanie stimulov a nájdenie správnej rovnováhy medzi spoluprácou a reguláciou v oblasti výmeny informácií, pokiaľ ide o mimoriadne udalosti a zraniteľnosti
    - Zváženie behaviorálnych aspektov bezpečnosti a súkromia
    - Preskúmanie príležitostí a rizík trhu v oblasti bezpečnosti informácií (napr. bug, zraniteľnosť, odhalenie informácií)
  - Vytvorenie modelov pre zavedenie nákladovo-efektívnych opatrení proti kybernetickým útokom a kybernetickej kriminálnej aktivite

DS-06-2017: Cryptography (RIA – dot. 100%)

- plánovaný termín otvorenia: 08.12.2016
- plánovaný termín uzávierky: 25.04.2017
- téma: Návrhy môžu riešiť jednu alebo viac oblastí popísaných nižšie, ale nemusia riešiť všetky z nich:
  - Funkčné šifrovacie riešenia, ktoré ponúkajú väčšiu flexibilitu, aby bolo možné spracovať šifrované dáta umiestnené na Internete. Výskum by sa mal zamerať na riešenie nad rámec

súčasných iba čiastkových homomorfných šifrovacích algoritmov, ktoré sú vo vývoji. Projekty by sa mali tiež vysporiadať s meraním úniku informácií, ak umožňujú flexibilitu a zachovanie dátových formátov. Navyše by sa mali zamerať na zníženie množstva únikov (napr. anonymizácia alebo zahmlievanie).
- Pre oblasti uplatnenia ako sú implantovateľné zdravotnícke prístroje a senzorové uzly, ktoré zbierajú energiu z okolia, je potrebná ultra-ľahká kryptológia. Mali by byť vytvorené dodatočné prostriedky na ochranu súkromia v týchto aplikáciách (napr anonymitu v komunikáciách)

DS-07-2017: Addressing Advanced Cyber Security Threats and Threat Actors (IA/RIA – dot. 70%/100%)

- plánovaný termín otvorenia: 01.03.2017
- plánovaný termín uzávierky: 24.08.2017
- téma: Výskum a inovácie – situačné povedomie
  - Zameranie návrhov by mal byť na vývoj nových prístupov na zabezpečenie situačného povedomia u organizácií vo vzťahu k hrozbám kybernetickej bezpečnosti, ktoré im umožnia odhaliť a rýchlo a účinne reagovať na sofistikované počítačové útoky.
  - žiadosti môžu využiť techniky, ako je detekcia anomálií, vizualizačných nástrojov, veľké analýzy dát, analýza hrozieb, kontrolu hlbokých paketov, analýzu protokolov, atď.
  - žiadosti by mali tiež zvážiť, že je potrebné zhromažďovať potrebné forenzné informácie o útočníkoch, ktoré môžu byť použité ako dôkaz v konaní pred súdom. Návrhy by mali posúdiť a riešiť dopady na základné práva, ochranu údajov a súkromia.
  - veľkosť projektu – 2-3 mil. EUR

  Inovačné opatrenia - Simulačné prostredie, školenia

  - Návrhy by mali rozvíjať inovačné simulačné prostredie a výukové materiály na adekvátnu prípravu tých, ktorí majú za úlohu brániť vysoko rizikové organizácie v boji proti pokročilým počítačovým útokom. Simulačné prostredia by mali vziať do úvahy nasledujúce výzvy:
  - Nástroje pre tvorbu realistických počítačových prostredí, ktoré zodpovedajú cieľom školenia a nástroje pre výrobu benígnych aj škodlivých systémových udalostí, ktoré zodpovedajú scenáru školenia
  - analýza výkonom študenta v reálnom čase, dynamická konfigurácia a prispôsobenie rozsahu cvičenia a náročnosti;
  - monitorovanie cvičenie a hodnotenie jeho stavu, schopnosť kontrolovať priebeh cvičenia, zisťovanie nezrovnalostí a riešenie náročných úloh, atď.;
  - definovanie a nákladovo a časovo efektívne vytvorenie nových scenárov a kybernetických hrozieb, čím sa lepšie dosiahnu pedagogické ciele pre širokú škálu profilov študentov;

  V kontexte kybernetického útokov, návrhy môžu tiež zvážiť vytváranie scenárov a simulačného výcviku na prípravu odozvy a rozhodovacích procesov v organizáciách v súvislosti s plnením ich zákonných povinností, alebo v širšom kontexte riadenia kríz a núdzových situácií.

DS-08-2017: Privacy, Data Protection, Digital Identities (IA – dot. 70%)

- plánovaný termín otvorenia: 01.03.2017
- plánovaný termín uzávierky: 24.08.2017
- téma: Žiadosti sa môžu vzťahovať aj na jednu z nižšie uvedených oblastí.

  Súkromie zvyšujúce technológie (PET)

  Nové návrhy a nástroje, ktoré poskytnú používateľom možnosť využívať funkcie, ktoré potrebujú, bez toho, aby odhalil nejaké ďalšie informácie, ako je potrebné, a bez toho, aby stratili kontrolu nad svojimi dátami v prospech tretích osôb. PET by mali byť k dispozícii v širokom spektre produktov a služieb, užívateľsky priateľské a prístupné. PET by mali byť tiež nákladovo-efektívne.

  Komplexné a konzistentné Rámce riadenia rizík ochrany súkromia by mali byť zahrnuté do projektov, s cieľom umožniť, aby ľudia pochopili dôsledky narušenia ochrany súkromia (t.j. pomáhať ľuďom pochopiť, čo sa deje s ich dátami, keď sú on-line, pomocou sociálnych sietí atď.) Open source a externe kontrolovateľných riešenie sa odporúča, aby sa maximalizovalo umiestnenie riešenia na trhu a zvýšila sa dôveryhodnosť navrhovaných riešení.

  Všeobecné nariadenie o ochrane údajov v praxi

Nástroje a metódy, ktoré pomôžu organizáciám implementovať GDPR, berúc do úvahy záverečné ustanovenia GDPR a príručky relevantných orgánov (úrady na ochranu údajov). Návrhy môžu tiež riešiť potrebu poskytnúť podporu organizáciám, aby pochopili, ako fungovať bez vyžadovania nepotrebných informácií (na podporu zavádzania posupov rešpktujúcich ochranu súkromia), konkrétne, ak je ich problémom, že vyžadujú od klientov príliš veľa informácií (podniky poskytovatelia služieb, vládne agentúry)

Secure Digital Identity

S cieľom znížiť množstvo krádeží identity a zároveň chrániť súkromie občanov, žiadosti by mali vytvoriť inovatívne, bezpečné a súkromie posilňujúce platformy pre digitálne identity nad rámec vnútroštátnych systémov EID.

Žiadosti môžu využiť existujúce Európske platformy elektronickej identifikácie a overovania s jasne definovanými rozhraniami na základe všeobecného nariadenia o ochrane údajov (GDPR).

CALL: FAST TRACT TO INNOVATION PILOT

https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ftipilot-2016.html#c,topics=callIdentifier/t/H2020-FTIPilot-2016/1/1/1&callStatus/t/Forthcoming/1/1/0&callStatus/t/Open/1/1/0&callStatus/t/Closed/1/1/0&+identifier/desc

FTIPilot-01-2016 Fast Tract to Innovation Pilot (IA – dot. 70%)

- plánovaný termín otvorenia: 02.12.2015
- plánovaný termín uzávierky: 15.03.2016, 01.06.2016, 25.10.2016

Cieľ výzvy:

Podpora zrýchlenia komercializačného procesu – teda uvádzanie nových výrobkov, postupov alebo služieb na trh

Podmienky konzorcia:

min. traja partneri z troch EÚ krajín

POZOR: konzorcia musia zahŕňať jedného partnera z oblasti priemyslu. Môžu sa zapojiť aj univerzity, výskumné a technologické organizácie. Je vítané zapojenie partnerov podporujúcich komercializáciu (napr. klastery, spotrebiteľské asociácie, inkubátory, investori a verejný sektor)

- zvýšený dôraz je kladený na firmy, ktoré sa prvýkrát zúčastnia programu HORIZONT

podmienky pre žiadosti:

- projekty v štádiu od demonštrácie po uvedenie na trh, vrátane pilotnej fázy, testovania, validácie a štandardizácie.
- zameranie na vyspelé nové technológie, koncepty, procesy a podnikateľské modely, ktoré potrebujú prejsť poslednou fázou pred uvedením na trh a dosiahnuť široké uplatnenie
- vítané sú medziodborové projekty
- ak je súčasťou projektu napr. technológia, musí byť na úrovni 6 technologickej vyspelosti (TRL 6), teda na úrovni technológie testovanej v relevantnom prostredí
- tematicky je potrebné byť v súlade so zameraním WP LEIT (Leadership in enabling and industrial Technologies) a/alebo prioritami tzv. Societal Challenges (spoločenské výzvy, napr. zdravie, potraviny, zdravé starnutie a pod.)
- súčasťou žiadosti je aj podnikateľský plán, zameraný na trhový potenciál, obchodné príležitosti a celkový prínos inovácie, vrátane aspektov ochrany duševného vlastníctva

Očakávané dopady:

- rýchly rozvoj, komerčné využitie a široké uplatnenie inovatívnych riešení (produktov, procesov, služieb, biznis modelov a pod.) v oblasti technológií alebo v oblasti špecifických spoločenských výziev (Societal challenges)
- uvedenie na trh do 3 rokov od začiatku projektu
- posilnenie konkurencieschopnosti a rastu komerčných partnerov v konzorciu (z hľadiska obratov a počtu zamestnancov)
- zvýšenie účasti priemyslu, vrátane malých a stredných podnikov v HORIZONTE, hlavne ak ide o prvú účasť

- v relevantných prípadoch aj nadnárodný prínos inovácie

CALL: SECURITY
https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-sec-2016-2017.html#c,topics=callIdentifier/t/H2020-SEC-2016-2017/1/1/1&callStatus/t/Forthcoming/1/1/0&callStatus/t/Open/1/1/0&callStatus/t/Closed/1/1/0&+identifier/desc

SEC-01-DRS-2016:Integrated tools for response planning and scenario building (IA – dot. 70%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Riziká katastrof (prírodných, náhodných alebo úmyselných) by mali byť riešené v kontexte:
  - Mechanizmu civilnej ochrany (Rozhodnutie 1313/2013), ktorý pripravuje cestu pre posilnenie spolupráce pri pomocných zásahoch civilnej ochrany pre ochranu predovšetkým osôb, ale aj životného prostredia a majetku v prípade prírodných a človekom spôsobených katastrof, núdzových situácií v prípade hromadných podujatí, teroristických činov a technologických, chemických, biologických, rádiologických a ekologických havárií
  - odporúčania IPCC (Medzivládny panel o klimatických zmenách) vo vzťahu ku klimatických udalostiam
  - Sendai Rámec pre zníženie rizík vzniku katastrof na medzinárodnej úrovni
  - Reakcie na núdzové situácie vyplývajúce z naplnenia týchto rizík vyžaduje medzi organizačnú spoluprácu medzi viacerými aktérmi a efektívna koordinácia vyžaduje zlepšenie plánovania odozvy a tvorbu scenárov. Toto je možné dosiahnuť len integráciou podporných nástrojov, ktoré môžu byť využité operatívne širokou paletou aktérov, back-office expertov a záchranárov.
- orientačná veľkosť projektu: 8 mil. EUR

SEC-03-DRS-2016: Validation of biological toxins measurements after an incident: Development of tools and procedures for quality control (IA – dot. 70%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Veľká variabilita medzi rodinami biologických toxínov komplikuje merania a jednoznačnú identifikáciu v ľudských vzorkách a vzorkách z prostredia alebo potravín. Toxíny sa rýchlo metabolizujú a degradujú po požití, čím sa obmedzuje časové okno pre úspešnú identifikáciu a forenznú analýzu. Žiadosti by mali rozvíjať nástroje kontroly kvality ako aj štandardné operačné postupy potrebné pre vytvorenie mechanizmu na systematické overovanie postupov laboratórnych meraní, vrátane stratégií pre prípravu vzoriek a analýz in-situ v mobilných alebo rýchlo nasaditeľných laboratóriách. Tieto nástroje by následne mali byť navrhnuté na schválenie na európskej úrovni.
- orientačná veľkosť projektu: 8mil. EUR

SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts (RIA – dot. 100%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Návrhy by sa mali zamerať len na jednu z týchto hľadísk:
  - Nové metódy pre ochranu davov počas masových zhromaždení
  - Nové metódy ako zabrániť, vyšetriť a zmierniť kriminálne správanie v kyberpriestore
  - Nové metódy, ako zabrániť, vyšetriť a zmierniť korupciu a finančnú kriminalitu v boji proti prenikaniu organizovaného zločinu do hospodárstva Európskej únie;
  - Nové metódy, ako zabrániť, vyšetriť a zmierniť veľký dopad drobnej trestnej činnosti;
  - Nové metódy, ako zabrániť, vyšetriť a zmierniť vysoký vplyv domáceho násilia
- orientačná veľkosť projektu: 3 mil. EUR

SEC-08-FCT-2016: Forensics techniques on: a) trace qualification, and b) broadened use of DNA (RIA – dot. 100%)

- plánovaný termín otvorenia: 15.03.2016

- plánovaný termín uzávierky: 25.08.2016

- téma: Forenzná komunita vyžaduje:
  a) V špecifickej oblasti kvality skúmania stôp:
  Lepšie znalosti o zložení stôp; o čase, keď boli zanechané, či sú výsledkom kriminálnej alebo neškodnej aktivity, vplyv času medzi zanechaním stôp a ich skúmaním na kvalitu stôp, o spôsobe prenosu stôp, odolnosť a obnovenie stôp
  Nové nástroje, ktoré majú byť použité v oblasti, ktorá môže odhaliť, zhromažďovať a analyzovať stopy, a pomáhajú pri interpretácii stopových dát s cieľom zabrániť predpojatosti všeobecného lekára;
  b) V špecifickej oblasti rozšíreného využívania DNA
  Nástroje a techniky a pokročilé metódy pre analýzu dát a štatistickú interpretáciu, ktoré by rozšírili možnosti využívania DNS, ktoré zavádzajú princíp „privacy by design" (ktoré berú do úvahy riešenie ochrany osobných údajov v členských štátoch EÚ).
  Nová metóda pre kompletné sekvencovanie a vytvorenie genetickej kompozitnej skice.
- orientačná veľkosť projektu: 5 mil. EUR

SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers´ networks (IA – dot. 70%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Návrhy by mali riešiť zavádzanie detekčných systémov vo veľkých a stredných mestách, v existujúcich sieťach, alebo kombináciu týchto sietí, napríklad pre detekciu prekurzorov výbušnín a nelegálnym chemikálií (drog). Žiadosti by sa mali zamerať na kanalizačné siete a siete pre kontrolu kvality ovzdušia, ale môžu riešiť aj ďalšie siete. Experiment by mal trvať relevantnú dobu (najmenej dva roky).
  Návrhy by mali tiež vytvoriť mobilnú platformu vybavenú pre zistenie zloženia a umiestnenie podozrivých vzoriek, ak boli dáta získané sieťových systémami detekcie.
  Návrhy by mali vytvoriť prototyp systému na kontrolu detekčných systémov schopného zlučovať dáta poskytnuté takýmito sieťami. Zvláštnu pozornosť je potrebné venovať etickým otázkam používania takýchto systémov, ako aj udržateľnosti týchto systémov.
  Vzhľadom k tomu, činnosti budú zamerané výhradne na civilné využitie, projekty môžu zahŕňať aj spoluprácu s Európskou obrannou agentúrou (EDA).
- orientačná veľkosť projektu: 8 mil. EUR

SEC-11-FCT-2016: Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot (RIA – dot. 100%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Inovatívne prístupy musia posúdiť účinnosti metód a techník používaných v boji proti ohrozeniu v určitom okamihu v čase sprisahania proti dôveryhodných scenárov založených na skutočných prípadoch; posúdiť, ako najlepšie kombinovať metódy a techniky na časovej osi sprisahania; identifikovať metódy a techniky schopné vyplniť existujúce medzery.
  Medzi metódy a techniky, ktoré je potrebné zvážiť, patria:
  - vyšetrenie na odhalenie tých, ktorí pripravujú útok;
  - zastavenie prekurzorov;
  - Detekcia špecifických chemikálií, tovární na výrobu bômb a / alebo IED;
  - Neutralizácia IED;
  - Identifikácia slabých miest súčasnej obrany proti IED, a možných zlepšeniach.
  Scenáre by mali brať do úvahy typ výbušnín (napr domáce, konvenčné) a prostriedky na tranzit a spôsob nasadenia, keďže oba faktory ovplyvňujú efektívnosť vybranej kombinácie metód alebo technológií. Nepredpokladá sa vývoj technológií, skôr operatívny výskum v spolupráci s odborníkmi. Výsledky akcie by mali slúžiť ako základ pre budúci rozvoj nových a inovatívnych techník detekcie výbušnín na dosiahnutie výraznej zmeny oproti súčasným metódam a technológiám.
  Vzhľadom k tomu, že žiadosti majú mať výhradne civilné využitie, je možná spolupráca s Európskou obrannou agentúrou (EDA)
- očakávaná veľkosť projektu: 5 mil. EUR

SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism (RIA – dot. 100%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Nové poznatky a cielené technológie na boj proti starým aj novým formám trestnej činnosti a teroristických správanie podporovanými pokročilými technológiami. Testovanie a demonštrácia novo vyvinutej technológie Aktérov presadzovania práva (LEA) zapojených do žiadostí. Inovatívne osnovy, školenia a (spoločné) cvičenia, ktoré majú byť použité pre uľahčenie zavádzania týchto nových technológií v celej EÚ, najmä v týchto oblastiach:
  1. kyber-zločin: virtuálne / crypto meny deanonymizácia / sledovanie / narušenia tam, kde podporujú podzemné trhy v čiernej zóne.
  2. Detekcia a neutralizácia zločinných / podozrivých ľahkých dronov/bezpilotných lietadiel letiacich nad uzatvorenými oblasťami, pričom je vhodné zapojiť do riešenia projektu aj relevantných prevádzkovateľov infraštruktúry
  3. video analýza v kontexte právneho vyšetrovania
  4. Ostatné. Návrhy v ďalších oblastiach sú vítané, za predpokladu, že zahŕňajú dostatočný počet orgánov presadzovania práva.

SEC-14-BES-2016: Smerom k zníženiu nákladov na technológie pozemnej hraničnej bezpečnostnej kontroly (RIA – dot. 100%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Náklady širokého spektra technológií by mohli byť cenovo dostupnejšie, prednostne tie, ktoré používajú na hraničných priechodoch nesúcich najťažšie bremeno (založený na analýze presunov ľudí a metód pašovania, súvisiacich rizík a prekážok v oblasti dohľadu a / alebo kontrola).Príslušné orgány hraničnej kontroly sú v najlepšej pozícii, aby identifikovali najdôležitejšie faktory dosiahnutia nákladovo efektívneho riešenia ochrany hraníc. Zníženie nákladov môže vyplývať zo: zlúčenia niekoľko pokročilých technológií do nových bezpečnostných riešení ochrany hraníc; zlepšenia pomeru cena-výkon; optimalizácie využívania technológií, ktoré sú najviac efektívne pre predchádzanie rizík v nadväznosti na konkrétne analýzy rizík; dosiahnutie väčšej interoperability medzi systémami včasným poskytovaním údajov. Žiadosti by mali vziať do úvahy dostupnosť alebo nedostatok ľudských zdrojov v priestoru, ako aj skutočnosť, že je potrebné poskytnúť prenosné a všestranné riešenia a zohľadniť viaceré parametre pre posúdenie pridanej hodnoty nových technológií. Najmä vytvorenie viac homogénnych IT platforiem, zdieľanie rozhrania spoločného pre všetky prevádzkové databázy a bezpečnostné aplikácie na ochranu hraníc, je žiaduce na zvýšenie efektívnosti riadenia ochrany hraníc.
- očakávaná veľkosť projektu 5 mil. EUR

SEC-15-BES-2017: Risk-based screening at border crossing (IA – dot. 70%)

- plánovaný termín otvorenia: 01.03.2017
- plánovaný termín uzávierky: 24.08.2017
- téma: Žiadosti by vziať do úvahy štvor-pilierový model riadenia prístupu vyvinutý v EÚ: 1. opatrenia prijaté v tretích krajinách alebo spoločne s tretími krajinami alebo poskytovateľmi služieb (napr. správcovia pokročilých informačných systémov s informáciami o cestujúcich - Advance Passenger Information alebo systémy zoznamov mien cestujúcich); 2. spolupráca so susednými krajinami; 3. hraničné kontroly a opatrenia proti pašerákom; 4. kontrolné opatrenia v oblasti voľného pohybu, aby sa zabránilo nelegálnemu prisťahovalectvu a cezhraničnej trestnej činnosti vo vnútri schengenského priestoru. Žiadosti môžu vyvíjať inovatívne medzinárodné výstražné systémy s cieľom posilniť spoluprácu pri presadzovaní práva a vyšetrovaní. Je dôležité stavať na znalostiach a skúsenostiach v tejto oblasti. Kombinácia rôznych senzorov, nových operačných metód a zlepšených postupov pri správe dát môže podporiť vhodné reakcie presadzovania práva a umožní lepšiu nadnárodnú spoluprácu a prístup k spoľahlivým a bezpečným spravodajským informáciám v reálnom čase a nákladovo-efektívnym spôsobom. Spolupráca s IATA, leteckým prepravným priemyslom a ďalšími partnermi a medzinárodnými zainteresovanými stranami v iných oblastiach bezpečnosti dopravy (napr. námornej, železničnej) môže viesť k vývoju nových riešení.

- očakávaná veľkosť projektu: 8 mil. EUR

SEC-16-BES-2017: Through-foliage detection, including in the outermost regions of the EUR (RIA – dot. 100%)

- plánovaný termín otvorenia: 01.03.2017
- plánovaný termín uzávierky: 24.08.2017
- téma: Mali by sa vypracovať systémy, ktoré kombinujú alebo zlepšujú technológie a postupy dohľadu a rôzne druhy senzorov, ktoré sú schopné poskytovať vyššiu kvalitu detekcie a zobrazovania prostredníctvom integrácie rôznych techník, aby sa dosiahlo širokouhlé alebo detailné zobrazenie lístia, aj napriek hustote porastu, v reálnom čase. Techniky by mohli stavať na vzdušných, družicových, a / alebo na pozemných platformách. Riešenia by mali byť testované a overené, pokiaľ ide o ich schopnosti účinne kontrolovať pozemnú hranicu pokrytú vegetačnou vrstvou, za všetkých poveternostných podmienok.

  Môže byť potrebné zahnúť do žiadosti predvýrobný výskum na riešenie rôznych štádií vývoja, od návrhu senzora, cez analýzu a návrh konfigurácie systému, a na jeho integráciu a validáciu zo strany (verejných) orgánov pri odhaľovaní, identifikácii a rozpoznaní cieľov.
- očakávaná veľkosť projektu: 8 mil. EUR

SEC-17-BES-2017: Architectures and organizations, big data and data analytics for customs risk management of the international goods supply chain trade movements (RIA – dot. 100%)

- plánovaný termín otvorenia: 01.03.2017
- plánovaný termín uzávierky: 24.08.2017
- téma: Riadenie rizík pohybu tovaru cez medzinárodné dodávateľského reťazca vyžaduje identifikáciu, vyhodnocovanie a analýzu celej škály rôznych hrozieb a rizík spojených s tovarom a jeho pohybom na úrovni EÚ, národnej a medzikontinentálne úrovni. Riadenie rizík začína s identifikáciou najzávažnejších rizík zo strany colných orgánov, tak aby potrebné kontroly boli vykonávané v najvhodnejšom čase a mieste.
  Sú potrebné vytvoriť stratégie a nástroje pre včasné vysoko-kvalitné a komplexné informovanie colných orgánov o tovare prepravovanom cez hranice, pri zohľadnení existujúcich národných a európskych predpisov, procedurálnych a informačných systémov. Je potrebné vyvinúť realistické metodiky a organizácie na uľahčenie spolupráce medzi príslušnými orgánmi (nielen colných, ale aj tých na vymáhanie práva, dopravných orgánov, bezpečnostných a hraničných kontrolných orgánov). Postupy a mechanizmy zdieľania dát musia byť medzinárodne dohodnuté.
  Spoločné úložiská, ktoré využívajú existujúce nástroje, akými sú informačný systém Advance Cargo (zaručené elektronické oznámenie o náklade prichádzajúcom do EÚ, pred tým, než opustí tretiu krajinu), ktoré sú málo a nedostatočne využívané pre účely riadenia rizík, môžu podporovať inteligentné využívanie a riadenie komplexných a objemných dát, využívanie neštruktúrovaných dát, podporu operatívneho a situačného povedomia colných orgánov, pridanie spravodajskej hodnoty informáciám (analýza trendov, korelačná analýza, atď.) pomocou dostupných technológií, vrátane oblasti Big Data, Data Analytics, Data Mining, vizualizácie, Intelligent User´s Interface, Insight knowledge and knowledge representation, umelej inteligencie, automatického jazykového prekladu. Je potrebné riešiť riadenie prístupu k týmto úložiskám.
- očakávaná veľkosť projektu: 5 mil. EUR

SEC-18-BES-2017: Acceptance of „no gate crossing point solutions"

- plánovaný termín otvorenia: 01.03.2017
- plánovaný termín uzávierky: 24.08.2017
- téma: Je potrebné posúdiť prijateľnosť (kombinácie) technológií a systémov zo strany občanov (ktorí potrebujú zachovať kontrolu osobných údajov) a praktikov, berúc do úvahy ľudské správanie, rod, právne rámce, spoločenské otázky a možné riziko diskriminácie. Je potrebné vyvinúť metódy pre vykonanie takéhoto hodnotenia, ktoré sú schopné generovať informácie užitočné pre proces rozhodovania, aby boli kompetentní prijímať informované rozhodnutia o nasadení budúcich technológií, a tiež, aby priemysel produkoval výrobky, ktoré zachovávajú súkromie.
- očakávaná veľkosť projektu: 3 mil. EUR

SEC-20-BES-2016: Bezpečnosť hraníc: autonómne systémy a kontrolné systémy (IA – dot. 70%)

- plánovaný termín otvorenia: 15.03.2016
- plánovaný termín uzávierky: 25.08.2016
- téma: Žiadosti by sa mali venovať jednej z nasledujúcich tém:
  1.Autonomný dohľad
  Autonómni agenti by mali byť adaptabilní: s cieľom vyrovnať sa s extrémnym a rozmanitým počasím a podmienkami na mori, a to aj v arktickom podnebí; mali by byť prepojení: interoperabilní a schopní prenášať dáta medzi sebou a zároveň s pozemnou časťou systému; tele-operabilné zo zeme. Mali by podporovať bezpečnostné misie od dohľadu až po odhalenie znečistenia mora, a to vrátane včasného zistenia a sledovanie nelegálnych aktivít a nelegálnej komunikácie. Mali by fungovať ako samostatné jednotky, ale aj ako homogénne alebo heterogénne skupiny, t.j. kombinovanie aerostatických, vzdušných dopravných prostriedkov so stabilnými, rotačnými krídlami (alebo tilt-rotor), bezpilotných povrchových vozidiel (USV), bezpilotných podzemných vozidiel (UUSV), bezpilotných pozemných vozidiel (UGV) s rôznymi typmi senzorov a komunikačných nástrojov na palube, prispôsobených pre prevádzkové a ekologické potreby. Autonómni agenti by si mali vymieňať informácie na taktickej úrovni a mali by komunikovať cez rozhranie medzi sebou navzájom a so systémom velenia a riadenia, ktoré sa v súčasnosti používajú na rôznych úrovniach.
  2. Posilnené riadiace a kontrolné systémy pre sledovanie hraníc v 3D prostredí autonómneho dohľadu
  Vylepšené riadiace a kontrolné systémy by mali zahrnúť:
  - Technológia kontroly vzdušného priestoru (vrátane radarovej technológie pre detekciu nízko letiacich lietadiel);
  - Pobrežné a podvodné hliadkovacie technológie (vrátane pobrežného radaru, námorných hliadkovacích lietadiel (MPA), ľahkých hliadkovacích lietadiel, bezpilotných lietadiel (UAV), hliadkovacích plavidiel, UUV, atď.);
  - Technológia pozemného dohľadu (vrátane UGV);
  - Satelitného služby;
  - Námorné informačné služby;
  - 3D kartografie a hĺbkové podmorské servery (bathymetry);
  - 3D modelovanie situačného obrazu založeného na 3D grafických ;
  - Technológie rozšírenej reality;
  - Mobilné zariadenia a telefóny, ako sú tablety a smartfóny
- očakávaná veľkosť projektov: 8 mil. EUR

verejne sprístupnené dielo MEDIA COELI ® podmienky: www.mediacoeli.sk