Rijksdienst voor Ondernemend Nederland

SBIR[1] Oproep, 17 april 2024

Autonoom delen van digitale dreigingsinformatie

Openingsdatum: 17 april 2024
Sluitingsdatum: 29 mei 2024

Budget : € 1.500.000

Het ministerie van Economische Zaken en Klimaat (EZK) daagt ondernemers uit om nieuwe producten en diensten te ontwikkelen om de innovatiedoelen van de Nederlandse Cybersecurity Strategie 2022-2028 (NLCS) te verwezenlijken. Vanuit deze strategie investeert het ministerie in het versterken van samenwerking, kennisontwikkeling en innovatie in cybersecurity via samenwerkingsplatformen dcypher en NEXIS, en via breed gedragen programma's, zoals CS4NL. In nauwe samenwerking met onderzoeksinstellingen, het bedrijfsleven en de Rijksoverheid worden projecten en activiteiten opgezet die Nederland cyberweerbaar en toekomstbestending maken.

Het ministerie richt haar activiteiten in het bijzonder op complexe cybersecurity uitdagingen, zoals het weerbaarder maken van vitale infrastructuren tegen digitale aanvallen, het eerder herkennen van kwetsbaarheden in software en hardware, het toekomstbestendig maken van encryptie technieken en het versterken van cybersecurity vaardigheden. Op deze, en andere gebieden, zijn innovaties nodig om voor te zorgen dat het Nederlandse bedrijfsleven bestand wordt tegen toekomstige cybersecurity incidenten.

Het samenwerken tussen bedrijfsleven, onderzoeksinstellingen en overheid om deze innovaties te realiseren is een elementair onderdeel van de NLCS. Het breed gedragen programma CS4NL richt zich op cybersecurity uitdagingen in de Nederlandse topsectoren zoals ketenveiligheid, veilige communicatie en OT/IT security en initieert, in samenwerking met de topsectoren, het ministerie van EZK en partners onderzoeksprojecten voor het MKB en kennisinstellingen.

Met deze SBIR oproep wil het ministerie een impuls geven aan innovatie op het gebied van het delen van cyberdreigingsinformatie en handelingsperspectieven daarop. Om de Nederlandse maatschappij weerbaarder te maken tegen cybersecurity aanvallen is het cruciaal dat informatie over dreigingen en tegenmaatregelen snel en goed gedeeld worden. Verschillende overheidspartijen en private actoren

[1] De afkorting SBIR komt van het Amerikaanse Small Business Innovation Research program. Het Amerikaanse SBIR programma is alleen toegankelijk voor kleine bedrijven. Het Nederlandse SBIR programma is toegesneden op kleinere ondernemingen, maar staat open voor iedereen, ook voor grote ondernemingen. SBIR behoort tot de zogeheten 'precommerciële' inkoop, de aanbestedingswet is hierop niet van toepassing. Wel geldt ook voor SBIR dat de procedure open, eerlijk en transparant is.

monitoren actief digitale aanvallen en nieuw herkende kwetsbaarheden in software, en delen deze informatie via open en gesloten kanalen. De laatste jaren is door de overheid en private partijen gewerkt aan het beter organiseren en coördineren van de informatiestromen over digitale dreigingen. Voor vitale sectoren zijn er al vertrouwde informatie gemeenschappen (ISACs), en tussen bedrijven en in sectoren zijn er waardevolle informatiegroepen ontstaan. De overheid stimuleert het breder en effectiever delen van cybersecurity informatie met de integratie van het NCSC, het CSIRT-DSP en het DTC. Hierbij is ook het programma Cyclotron van belang, waarin een platform ontwikkeld gaat worden waarbinnen publieke en private partijen informatie delen over digitale incidenten en dreigingen. Deze ontwikkelingen gaan gestaag en laten vooralsnog veel ruimte over voor verbetering, met name in de informatie naar belanghebbenden die geen vanzelfsprekende IT- of cybersecurity capaciteit hebben, zoals niet-technische MKB en maatschappelijke organisaties. Een groot deel van deze organisaties zal voorlopig een zwakkere informatiepositie blijven houden, en daarnaast ook geen goed handelingsperspectief hebben bij incidenten.

De aankomende NIS2 richtlijn gaat een grotere groep bedrijven aanspreken op hun verantwoordelijkheid om digitaal veilig te werken en om incidenten te melden. Het voldoen aan deze strengere normen gaat veel van bedrijven vergen en het belang van een sterke informatiepositie verduidelijken. Naast organisatorische maatregelen, zoals het 'Cyberweerbaarheidsnetwerk' dat de overheid aan het opbouwen is, kunnen technologische instrumenten hierbij helpen. Denk aan systemen die helpen in de verspreiding van dreigingsinformatie en bedrijven voorzien van advies tot handelen.

Om deze redenen wil het ministerie van EZK bedrijven uitnodigen om innovatieve oplossingen voor te stellen die een bijdrage leveren aan het versterken van de cybersecurity informatievoorziening, met name gericht op het verbreden van de reikwijdte van informatie en het vertalen van informatie naar de context, capaciteit en competenties van ontvangers van deze informatie.

SBIR is een innovatie-competitie om ondernemers uit te dagen om nieuwe producten of diensten te ontwikkelen gericht op de aanpak van een maatschappelijk vraagstuk. Wij zijn op zoek naar concreet bruikbare toepassingen, die onder andere kunnen worden gebruikt door (semi-) publieke organisaties. De overheid is daarbij een potentiële (maar geen exclusieve) inkoper.

1. Doel van deze SBIR-competitie

Nederlandse bedrijven en overheidsinstanties krijgen steeds meer te maken met de effecten van digitale verstoringen. Statelijk actoren en criminelen worden steeds inventiever in hun aanvallen en veroorzaken steeds meer verstoringen en economische schade. Het is daarom essentieel dat informatie over dreigingen, aanvalsmethodes, kwetsbaarheden en verdedigingsmethodes zo snel mogelijk en zo veel mogelijk gedeeld worden. Een sterke informatiepositie voorkomt verrassingsaanvallen.

In deze oproep nodigen wij bedrijven uit om innovatieve producten en diensten te ontwikkelen waarmee er meer en pro-actievere informatiedeling ontstaat tussen bedrijven en overheidspartijen over cybersecurity dreigingen. Hierbij voorzien we een informatienetwerk waarbij niet de gebruikers informatie ophalen of verzenden, maar het netwerk zelf de informatie brengt naar waar het relevant is. Daarbij wordt informatie proactief door het systeem aangepast zodat er geen gevoelige informatie gedeeld wordt, maar wel 'actionable intelligence'. We zoeken technologie en prototypes die kunnen laten

zien dat informatie over cybersecurity risico's, tegenmaatregelen en ontwikkelingen sneller en breder gedeeld worden, met bescherming van de partij die de informatie deelt en vormgeving naar wat de ontvanger nodig heeft om te handelen.

1.1 Randvoorwaarden

Alvorens te worden beoordeeld op de 3 criteria van paragraaf 4 dient de indiener in de offerte aannemelijk te maken dat de innovatie gedemonstreerd kan worden in een realistische setting, en onder verschillende scenario's aan het einde van fase 2 van deze SBIR.

2. Procedure

SBIR is een open competitie voor iedere marktpartij die innovatieve (technologische) oplossingen voor maatschappelijke vraagstukken kan ontwikkelen. De SBIR-systematiek kent twee fasen:

1. Fase 1: haalbaarheidsonderzoek.
2. Fase 2: prototype-ontwikkeling en eerste praktijktesten.

Een onafhankelijke commissie zal de Rijksdienst voor Ondernemend Nederland (RVO) en het ministerie van EZK adviseren welke voorstellen voor producten en diensten (SBIR fase 1) het beste aan de criteria voldoen. De beste voorstellen krijgen een opdracht. Partijen die met goed resultaat het fase 1 haalbaarheidsonderzoek hebben afgerond, kunnen, op verzoek, een aanbod doen voor SBIR fase 2 (het onderzoeks- en ontwikkelingstraject). Ook bij deze tweede fase zal een onafhankelijke commissie adviseren. Vervolgens krijgen de partijen met de beste offertes voor fase 2 een opdracht om hun product verder te onderzoeken en te ontwikkelen tot een (ruw) prototype.

RVO voert namens het ministerie van EZK deze opdracht uit.

3. Budget

Het ministerie van EZK stelt voor fase 1 van deze SBIR in totaal een budget van maximaal € 400.000 (incl. btw) beschikbaar. Het maximumbedrag per haalbaarheidsonderzoek (fase 1) bedraagt € 30.000 (incl. btw).

Voor SBIR fase 2 is maximaal € 1.100.000 (incl. btw) beschikbaar, het maximumbedrag per project is € 200.000 (incl. btw).

Het precieze aantal te honoreren projecten voor fase 1 en fase 2 hangt af van de prijs van de best beoordeelde offertes voor fase 1 en 2. Alleen de projecten die met goed resultaat het haalbaarheidsonderzoek in fase 1 hebben afgerond kunnen worden uitgenodigd om voor fase 2 een aanbod te doen.

Het aantal te honoreren projecten voor de verschillende fasen is afhankelijk van de prijs en de kwaliteit van de best beoordeelde offertes per fase. Overblijvend budget uit fase 1 kan in fase 2 worden ingezet. SBIR vergoedt alleen kosten voor onderzoek en ontwikkeling. De marktintroductie is geen onderdeel van SBIR.

4. Beoordeling

De beoordeling vindt plaats conform de in de SBIR handleiding beschreven procedure (versie maart 2021): https://www.rvo.nl/subsidies-financiering/sbir-innovatie-opdracht/offertes-indienen (onderaan de pagina).

Alleen projectvoorstellen die voldoen aan de randvoorwaarden worden verder beoordeeld.

Bij de beoordeling (totaal maximaal 100 punten te behalen) is per criterium maximaal het volgende aantal punten toe te kennen:

1. Impact: 40
2. Technologische haalbaarheid: 30
3. Economisch perspectief: 30

Alleen projecten die 60% of meer van het maximaal aantal punten op alle criteria scoren, worden in de rangschikking opgenomen om voor een opdracht in aanmerking te komen.

Wij moedigen aanbiedingen aan waarin de verhouding tussen impact en prijs zo gunstig mogelijk is, zodat het budget zo efficiënt mogelijk wordt ingezet.

4.1 Impact

In aanvulling op de criteria in de handleiding scoort een voorstel bij het criterium 'Impact' hoger naarmate:

- de innovatie meer gericht is op een of meerdere van de volgende functionaliteiten:
  - Automatisch voorzien van organisaties van passende informatie over dreigingen en tegenmaatregelen via digitale informatiesystemen (denk aan *fingerprinting*);
  - Ondersteuning van menselijke actoren in het opstellen, uitvoeren en monitoren van informatie-activiteiten met intelligente, (zelf)lerende, interacterende hulpsystemen;
  - Ondersteunende, zelflerende systemen die organisaties helpen om gedeelde informatie te interpreteren, operationaliseren en evalueren (planvorming, tracking en uitvoering van cyberweerbaarheidsadviezen);
  - Het mogelijk maken dat sensitieve dreigingsinformatie eenvoudiger gedeeld kan worden in zowel vertrouwde informatiegroepen, open netwerken en naar relevante bedrijven, door deelinformatie weg te laten uit de berichtgeving, of te vertalen zodat een grotere groep belanghebbenden geïnformeerd kan worden zonder veiligheids- of bedrijfseconomische belangen te schaden.

- de innovatie vergezeld gaat van een duidelijke uitleg hoe het meerwaarde creëert ten opzichte van de huidige praktijk van cybersecurity informatiedeling;
- het systeem beter kan uitleggen wat het gedaan heeft, en waarom (explainability). Hierbij is het voorkomen van *bias* en *preselectie* belangrijk.

4.2 (Technologische) haalbaarheid

In aanvulling op de criteria in de handleiding scoort een voorstel bij het criterium '(Technologische) haalbaarheid' hoger naarmate:

- het product of de dienst beter inpasbaar is als maatwerk binnen veelgebruikte softwareomgevingen, zoals ticketsystemen (of als vervanging daarvan kan functioneren);
- er sprake is van meer automatisering/autonomie: kan het op te leveren prototype autonoom worden ingezet of is (veel) interactie met een menselijke operator nodig? Welke inspanning en doorlooptijd zullen nodig zijn om het prototype te configureren of trainen?;
- er sprake is van meer gebruikersgemak. Welke expertise en ervaring van de gebruiker wordt verondersteld om het prototype effectief te kunnen inzetten en hoe intuïtief zal de gebruikersinterface zijn?;
- het product of de dienst beter passend is binnen de huidige en verwachte wetgeving;
- de technische opbouw en werking van het product duidelijk wordt gemaakt in het projectplan;
- het product of de dienst betrouwbaar en transparant is in zijn werking.

4.3 Economisch perspectief

In aanvulling op de criteria in de handleiding scoort een voorstel bij het criterium 'Economisch perspectief' hoger naarmate:

- de voorgenomen aanpak en strategie om het product een plaats in de markt te bezorgen beter is;
- de kansen in de Nederlandse markt beter zijn (herhaalpotentieel);
- het product of dienst beter toepasbaar is binnen Europa;
- er meer gebruik wordt gemaakt van internationale dreigingsinformatie;
- de mate waarin de potentiële eindgebruikers bij de ontwikkeling betrokken zijn;
- het product of de dienst schaalbaar is;
- het product toepasbaar is in urgente en normaalsituaties.

5. Informatiebijeenkomst

Op 1 mei 2024 organiseert RVO een informatiebijeenkomst in Den Haag. Deze zal zowel fysiek als online zijn. Verdere informatie hierover is binnenkort te lezen op de website van RVO.

U kunt zicht hiervoor aanmelden via een digitaal aanmeldingsformulier. De aanmeldknop staat op de pagina van de oproep op de website van RVO.

Het programma van de informatiebijeenkomst ziet er globaal als volgt uit:

- 13:45 tot 14:00 uur: Inloop
- 14:00 tot 15:30 uur: Presentaties van het ministerie van EZK over de maatschappelijke uitdaging, RVO (SBIR procedure en Octrooicentrum) en gelegenheid tot het stellen van vragen
- 15:30 tot 16:30 uur: Napraten en netwerken met een drankje

6. Informatie en contact

6.1. Vragen

Vragen met betrekking tot deze SBIR-competitie (tot maximaal 10 dagen voor sluitingsdatum) kunt u sturen naar: sbir@rvo.nl

Alle informatie over deze SBIR-competitie en relevante SBIR-documenten staat op de volgende websites:

- http://www.rvo.nl/subsidies-regelingen/sbir – de oproep, presentaties na de voorlichtingsbijeenkomst, de nota van inlichtingen en eventuele aanvullende (achtergrond-)info.
- https://mijn.rvo.nl/sbir-innovatie-in-opdracht – de formats voor het indienen van de offerte.

Indienen offertes (projectvoorstellen fase 1)

U dient uw offerte voor fase 1 in via het online SBIR formulier. De contactpersoon (en indien van toepassing uw intermediair) ontvangt een automatisch gegenereerde ontvangstbevestiging met de ingezonden stukken. Een kopie hiervan gaat naar sbir@rvo.nl. De offerte dient uiterlijk op 29 mei 2024 om **17:00** uur in het bezit te zijn van RVO.

Een volledige SBIR-offerte bestaat uit:

- het ingevulde online SBIR-formulier
- het projectplan voor fase 1 incl. de begroting
- de managementsamenvatting

Upload de bestanden als aparte PDF-, Word- of Excelbestanden via het online SBIR formulier.

Wij raden u aan om een aantal werkdagen voor de deadline uw offerte in te dienen.

Let op: dien uw offerte tijdig in. Te laat *ontvangen* offertes worden niet meegenomen in de beoordeling. De grootte van de bijlages is gelimiteerd tot 4MB per bestand. Voor grotere bestanden kunt u via sbir@rvo.nl een beveiligde link opvragen om uw bestand te uploaden.

Het is niet mogelijk om de offerte via TenderNed in te dienen.

Planning

Openstelling tender	17 april 2024
Informatiebijeenkomst	**1 mei 2024**
Sluiting indienen fase 1 offertes	**29 mei 2024 om 17.00**
Commissievergadering; toelichten offerte	17 juni 2024
Bekendmaking uitslag	21 juni 2024
Opdrachtverstrekking fase 1	5 juli 2024
Einddatum haalbaarheidsrapport + indienen offerte fase 2	10 januari 2025
Commissievergadering; toelichten offerte	27 januari 2025
Bekendmaking uitslag fase 2	31 januari 2025
Opdrachtverstrekking fase 2	19 februari 2025
Deadline eindrapport fase 2	19 februari 2026

RVO behoudt zich het recht voor om bijgevoegd tijdspad indien nodig aan te passen. Dit zal tijdig aan (potentiële) opdrachtnemers worden gecommuniceerd.

Dit is een publicatie van:

Rijksdienst voor Ondernemend Nederland
Prinses Beatrixlaan 2 | 2595 AL Den Haag
Postbus 93144 | 2509 AC Den Haag
T +31 (0) 88 042 42 42
Publicatienummer: RVO-076-2024/BR-INNO
Contact
www.rvo.nl