Adviescollege ICT-toetsing

> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Buitenlandse Zaken
t.a.v. de minister, de heer drs. C.C.J Veldkamp
Postbus 20061
2500 EB Den Haag

Afschrift aan: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
t.a.v. de staatssecretaris Digitalisering en Koninkrijksrelaties, de heer drs. F.Z. Szabó
Postbus 20011
2500 EA Den Haag

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
adviescollegeicttoetsing.nl

Contactpersoon
info@adviescollegeicttoetsing.nl

Datum
3 februari 2025

Kenmerk
2025-0000122205

Uw kenmerk
BZ2511681

Betreft
Advies programma Transitie ICT-dienstverlening

Geachte heer Veldkamp,

U heeft het Adviescollege ICT-toetsing verzocht een onderzoek uit te voeren naar het programma Transitie ICT-dienstverlening van het ministerie van Buitenlandse Zaken (BZ). De opdrachtgever is de plaatsvervangend secretaris-generaal van uw ministerie. Dit advies sturen we tevens in afschrift aan de staatssecretaris Digitalisering en Koninkrijksrelaties, omdat de onderwerpen die aan bod komen ook betrekking hebben op onderdelen of beleidsterreinen van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK).

Het advies kan als volgt worden samengevat:

Het ministerie van Buitenlandse Zaken (BZ) heeft een deel van de ICT-dienstverlening bij het Shared Service Center (SSC)-ICT belegd, net als acht andere ministeries. SSC-ICT is een onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Met het nog te starten programma Transitie ICT-dienstverlening beoogt BZ invulling te geven aan een eerder besluit van BZ om te vertrekken bij SSC-ICT en de ICT-dienstverlening te beleggen bij een andere partij.

Conclusie

De belangrijkste conclusie uit het onderzoek is dat wij het besluit van BZ om nu te vertrekken bij SSC-ICT te risicovol vinden, zowel vanuit het perspectief van BZ als vanuit het rijksbrede belang, want:

A. Vertrek brengt de urgente verbetering van de informatiebeveiliging in gevaar.
B. Grote kans op herhaling problematiek dienstverlening door onvolwassen besturing BZ.
C. Vertrek belemmert noodzakelijke beveiliging tegen statelijke actoren voor BZ en rijksbreed.

Advies

Wij adviseren om het vertrekbesluit nu niet door te zetten. Geef eerst de urgente verbetering van de huidige ICT-dienstverlening topprioriteit:

1. Zorg dat SSC-ICT en BZ de urgente beveiligingsrisico's terugdringen.
2. Zorg dat de besturing bij BZ fundamenteel verbetert.
3. Realiseer vanuit BZK een rijksbrede aanpak beveiliging tegen statelijke actoren.
4. Evalueer na twee jaar gezamenlijk de opvolging van de adviezen.

Hieronder vindt u eerst een korte beschrijving van het programma Transitie ICT-dienstverlening. Daarna werken we bovenstaande analyse en adviezen nader uit. Wij concentreren ons hierbij op de belangrijkste risico's. In de bijlage vindt u de details van het programma.

Adviescollege ICT-toetsing

Datum
3 februari 2025

Kenmerk
2025-0000122205

Korte omschrijving van het programma Transitie ICT-dienstverlening

Vóór 2015 had BZ een eigen ICT-afdeling. Sinds 2015 maakt BZ gebruik van de ICT-dienstverlening van het Shared Service Center (SSC)-ICT. Bij de overgang naar SSC-ICT heeft BZ circa 100 medewerkers overgedragen. SSC-ICT levert diensten voor werkplekken, housing (fysieke huisvesting van de datacentra) en hosting (alle specifieke hard- en software, inclusief de technische beheeractiviteiten), en verzorgt het beheer van applicaties. SSC-ICT doet dat zowel in Nederland als wereldwijd, op 160 posten en voor drie datacentra in Nederland, Singapore en Noord-Amerika. De directie Informatievoorziening en Digitale Innovatie (IDI) van BZ is verantwoordelijk voor de regievoering op SSC-ICT.

SSC-ICT bestaat sinds 2014. Het is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en opgericht om te zorgen voor meer efficiëntie en samenwerking binnen de rijksoverheid. Negen ministeries maken gebruik van de ICT-dienstverlening van SSC-ICT. Vanuit de gedachte van 'gedeelde diensten' ligt de nadruk bij SSC-ICT op standaarddienstverlening. De ICT-dienstverlening voor BZ wijkt hiervan af omdat BZ wereldwijd werkt, te maken heeft met verhoogde dreiging van statelijke actoren en moet voldoen aan accreditatie-eisen vanuit de Europese Unie (EU) en de NAVO. BZ stelt daarom specifieke eisen, zoals een afgescheiden netwerk, specifieke cryptovoorzieningen en toepassing van BasisBeveiligingsNiveau 3 (BBN3) uit de Baseline Informatiebeveiliging Overheid (BIO)[1] voor de systemen en infrastructuur waar departementaal vertrouwelijke informatie wordt verwerkt.

BZ en SSC-ICT hebben al lange tijd een moeizame onderlinge samenwerking om een aantal redenen, waaronder:

- Er is geen gedeeld beeld van de invulling van de dienstverleningsafspraken. SSC-ICT houdt, in de ogen van BZ, onvoldoende rekening met de eisen en wensen van BZ. In de ogen van SSC-ICT vult BZ het opdrachtgeverschap niet volwassen in.
- Gezamenlijke initiatieven die de afgelopen jaren zijn gestart om de dienstverlening en de beveiliging te verbeteren, hebben niet altijd de gewenste resultaten opgeleverd.
- In 2023 waren er meerdere beveiligingsincidenten die tot verschil van mening leidden. SSC-ICT en BZ dachten niet alleen verschillend over de invulling van hun rol bij deze incidenten, maar ook over noodzakelijke verbetering van de beveiliging.
- Sinds de overgang van BZ naar SSC-ICT in 2015 zijn de ICT-systemen op posten en in datacentra beperkt vernieuwd. Een langlopende discussie over de toerekening van de kosten van de vernieuwing is pas recent afgerond, waardoor de vernieuwing flink is vertraagd.

Eind 2023 heeft BZ eenzijdig besloten om te vertrekken (te 'ontvlechten') bij SSC-ICT. De toenmalige minister van BZ heeft aan de toenmalige staatsecretaris van Digitalisering en Koninkrijksrelaties meegedeeld een 'herziening van de dienstverlening door SSC-ICT aan BZ voor te bereiden'. Dit is in januari 2024 mondeling en in juni 2024 schriftelijk gebeurd. De staatssecretaris heeft hierop nog niet schriftelijk gereageerd.

De invulling van het besluit is door BZ nog niet bepaald. Zo moet BZ nog bepalen of het vertrek voor de hele ICT-dienstverlening geldt of alleen voor de 'kritieke diensten' (waaronder werkplek, housing, specifieke applicaties, crypto-apparatuur en het postennetwerk).

[1] De BIO definieert 3 basisbeveiligingsniveaus (BBN's). BBN2 is het standaardniveau voor de Rijksoverheid. BBN3 vergt aanvullende maatregelen, op basis van organisatiespecifieke risicoanalyses, om weerstand te kunnen bieden tegen statelijke actoren en criminele organisaties. Deze maatregelen of het proces om deze te selecteren zijn niet in de BIO geconcretiseerd.

BZ heeft een eerste projectbrief opgesteld waarin de contouren van het programmaplan Transitie ICT-dienstverlening staan. Een scenario-analyse en een businesscase worden momenteel uitgewerkt. De eerste grove inschatting van BZ is dat de transitie naar een nieuwe dienstverlener vijf jaar gaat duren. Er is nog geen kosteninschatting gemaakt. BZ wil dat lopende en geplande verbeter- en vernieuwingsprojecten bij SSC-ICT gedurende de transitie doorgaan.

BZ neemt niet alleen diensten van SSC-ICT af, maar ook van private aanbieders; bijvoorbeeld een 'Hoog Beveiligde Omgeving (HBO)' van Atos (de huidige HBO1) en Capgemini (de nieuwe HBO2 en Azure cloud). Daarnaast levert British Telecom de netwerkconnectiviteit met de posten.

Conclusie: Doorzetten vertrekbesluit te risicovol

Vanwege de internationale context en de dreiging van statelijke actoren is het noodzakelijk dat de ICT-dienstverlening voor BZ – inclusief de beveiliging – goed op orde is. Dit stelt hoge eisen aan dienstverlener SSC-ICT, aan de besturing vanuit BZ én aan hun onderlinge samenwerking. Beide partijen voldoen nu niet in voldoende mate aan die eisen.

Ondanks meerdere verbeterpogingen in de afgelopen jaren is er, gezien de moeizame relatie tussen beide partijen, weinig concreet perspectief dat de huidige situatie structureel gaat verbeteren. Desalniettemin vinden wij het besluit van BZ om te vertrekken bij SSC-ICT te risicovol, zowel vanuit het perspectief van BZ als vanuit het rijksbrede belang. Wij hebben hiervoor de volgende redenen.

A. Vertrek brengt urgente verbetering informatiebeveiliging in gevaar

De eerste inschatting van BZ is dat de transitie naar een andere dienstverlener vijf jaar gaat duren. BZ en SSC-ICT zitten dus nog een aantal jaren aan elkaar vast. De transitieperiode zal veel schaarse capaciteit en aandacht van zowel SSC-ICT als BZ vergen. Hierdoor is de beschikbare capaciteit beperkt om urgente beveiligingsrisico's in de BZ-dienstverlening vanuit SSC-ICT terug te dringen.
Gezien de aard van deze risico's zijn ze niet in dit publieke advies opgenomen maar in een vertrouwelijke bijlage met een beperkte verspreidingskring.

B. Grote kans herhaling problematiek dienstverlening door onvolwassen besturing BZ

Wij denken dat BZ te optimistisch is over wat de transitie naar een andere ICT-dienstverlener aan verbetering zal brengen. De huidige situatie is namelijk mede ontstaan omdat BZ niet voldoende is toegerust om de besturing van het ICT-domein goed in te richten. Met een transitie naar een nieuwe ICT-dienstverlener is de kans groot dat de problemen met de huidige dienstverlening zich herhalen. Wij constateren het volgende:

- BZ is onvoldoende in staat om concrete eisen aan de ICT-dienstverlening te stellen:
  - De uitvoering van het risicomanagement is niet op orde. BZ kan onvoldoende scherp afbakenen wat voor BZ de kritieke processen en informatiestromen zijn, wat hun dreigingsniveau is en hoe ze zich verhouden tot de verschillende ICT-diensten. Hierdoor kan BZ niet goed bepalen welke ICT-diensten aan een hoger beveiligingsniveau moeten voldoen.
  - BZ stelt eisen op een te hoog abstractieniveau. De specifieke internationale context van BZ vraagt om duidelijke eisen voor leveranciers, zodat zij de mogelijkheid krijgen om de ICT-dienstverlening passend in te richten. BZ is onvoldoende in staat om die eisen concreet te formuleren, waardoor de kans groot is dat dit bij een nieuwe ICT-

dienstverlener opnieuw leidt tot stroeve discussies, misinterpretatie en verschillende verwachtingen.

- De regievoering vanuit BZ op dienstverleners staat nog in de kinderschoenen:
  - Elementaire zaken ontbreken, zoals inzicht in welke ICT-diensten BZ nu precies afneemt van welke dienstverlener of leveranciers. Daarnaast ontbreekt het aan effectieve centrale coördinatie en prioriteitsstelling van opdrachten aan dienstverleners. Daardoor heeft de aansturing in hoge mate een ad hoc karakter.
  - BZ acteert weinig rolvast waardoor samenwerking met SSC-ICT stroef en onvoorspelbaar verloopt. BZ verwacht enerzijds dat de dienstverlener als 'goed huisvader' diensten levert, maar behandelt de dienstverlener anderzijds als een interne IT-afdeling door specifieke ICT-oplossingen voor te schrijven.
- De uitvoering van de interne beveiligingsprocessen bij BZ is niet op orde:
  - BZ leeft haar eigen beveiligingsbaseline onvoldoende na. Zo ontbreekt het bijvoorbeeld aan een sluitend intern auditproces om periodiek de naleving van de beveiligingskaders vast te stellen en verbetermaatregelen te identificeren. Daarnaast is er bij de afhandeling van een significant beveiligingsincident geen onderzoek gedaan naar de grondoorzaak.
  - BZ heeft het accreditatiebeleid onvolledig geïmplementeerd voor systemen waarin nationaal of internationaal (EU/NAVO) gerubriceerde informatie wordt verwerkt. Bij de beoordeling van deze systemen moeten minimaal de relevante (technische) beveiligingskaders als criteria zijn meegenomen, zoals bijvoorbeeld de BIO BBN2-maatregelen. In de praktijk blijkt echter dat dit niet voldoende gebeurt. Bij de beoordeling van de werkplek- en de basis ICT-infrastructuur zijn maatregelen op BBN2-niveau uit de BIO niet expliciet meegenomen.

C. Vertrek belemmert noodzakelijke beveiliging tegen statelijke actoren voor BZ en rijksbreed

Meerdere organisaties binnen de rijksoverheid worstelen – net als BZ – met de beveiliging tegen statelijke actoren en criminele organisaties (BBN3). Daarbij constateren wij dat deze organisaties grote moeite hebben om de benodigde maatregelen in de systemen en infrastructuur te treffen. Bovendien wordt dit vraagstuk urgenter. Zo blijkt uit het Cybersecuritybeeld 2024[2] dat statelijke actoren hun activiteiten in Nederland intensiveren. Ze verbreden daarbij hun capaciteiten, mede door samen te werken met cybercriminelen. Ook zorgt de internationalisering van de IT-markt ervoor dat rijksorganisaties steeds meer afhankelijk worden van buitenlandse leveranciers. Deze hebben dikwijls te maken met andere wetgeving en daar is lastiger toezicht op te houden.

Wij vinden dat een rijksbrede aanpak noodzakelijk is om BBN3 ICT-dienstverlening voor rijksorganisaties, waaronder BZ, goed in te vullen. Wij verwachten dat een vertrek van BZ bij SSC-ICT de totstandkoming van zo'n rijksbrede aanpak belemmert. Wij hebben hiervoor de volgende redenen:

- Voor het ontwerp van BBN3 ICT-dienstverlening moet schaarse specialistische kennis bij verschillende delen van de rijksdienst gebundeld worden. Het gaat om kennis over de modus operandi van aanvallers en over beveiligingstechnieken. Rijksbrede, goede voorbeelden dragen bij aan verdere kennisopbouw. Ter illustratie: specifieke expertise op dit gebied van de AIVD, MIVD en het Nationaal Cyber Security Centrum (NCSC) is schaars. Inbreng vanuit BZ is essentieel gezien de ervaring en de specifieke landenkennis.
- De realisatie van BBN3 ICT-dienstverlening vergt aanzienlijke beheerinvesteringen, bijvoorbeeld in een gespecialiseerd 24/7 *Security Operations Center* (SOC), de ontwikkeling van een BBN3-werkplek en toepassing van cryptografische technieken. Deze investeringen

[2] Zie het NCTV "Cybersecuritybeeld Nederland 2024", beschikbaar op www.nctv.nl.

zijn voor rijksorganisaties zeer kostbaar om individueel te dragen. Dienstverlening wordt zo veel duurder dan nodig. Bovendien ligt een gezamenlijke investering in lijn met de ambitie om ICT-dienstverlening binnen de rijksoverheid te consolideren.

Advies: Geef urgente verbetering van huidige ICT-dienstverlening topprioriteit

Wij adviseren om het vertrekbesluit nu niet door te zetten. Geef eerst de urgente verbetering van de huidige ICT-dienstverlening topprioriteit. Wij hebben daartoe een aantal adviezen geformuleerd.

Randvoorwaardelijk voor de opvolging van deze adviezen is dat BZ en SSC-ICT eerst tot een goede samenwerkingsrelatie komen, met wederzijds respect en begrip voor elkaars situatie en (on)mogelijkheden. Ook moeten beide partijen de intentie hebben om samen de gesignaleerde problematiek op te lossen. Daarvoor is een reset nodig van de huidige relatie op alle niveaus, maar vooral op strategisch en tactisch niveau. Wij kunnen ons voorstellen dat een door beide partijen geaccepteerde onafhankelijke partij een bemiddelende rol bij deze reset vervult. Het is van belang dat de eigenaar van SSC-ICT de ruimte voor deze reset biedt, zeker in het besef dat een groot deel van de te nemen acties ook waardevol zijn voor de andere aan SSC-ICT deelnemende ministeries.

1. Zorg dat SSC-ICT en BZ samen urgente beveiligingsrisico's terugdringen

Gezien de urgente beveiligingsrisico's is het noodzakelijk dat BZ en SSC-ICT constructief gaan samenwerken om de risico's op korte termijn terug te dringen. Wij adviseren om maatregelen te treffen en over de voortgang ervan iedere drie maanden aan de minister van Buitenlandse Zaken en aan de staatssecretaris Digitalisering en Koninkrijksrelaties te rapporteren.
Gezien de aard en details van de maatregelen die wij adviseren, zijn deze niet in dit publieke advies opgenomen maar in een vertrouwelijke bijlage.

2. Zorg dat de besturing bij BZ fundamenteel verbetert

Om tot een meer professionele omgang met ICT-dienstverleners te komen, is het noodzakelijk dat BZ de besturing van het ICT-domein fundamenteel verbetert. Wij adviseren BZ om de volgende maatregelen te treffen:

- Werk de eisen voor de ICT-dienstverlening – inclusief beveiliging – beter uit:
  - Richt een sluitend risicomanagementproces in. Breng de kritieke processen en informatiestromen en bijbehorend dreigingsniveau voor BZ in kaart. Definieer op basis daarvan de specifieke beveiligingsbehoefte.
  - Verbeter het proces voor de specificatie van eisen aan dienstverleners. Stel op basis van de beveiligingsbehoefte duidelijke eisen op waarin de internationale context van BZ en het bijbehorende dreigingsbeeld is meegewogen.
- Breng de regievoering op orde:
  - Verbeter de inrichting van het contractmanagement van BZ, zodat het maken, bewaken en bijsturen van afspraken volgens een gestructureerd en beheerst proces plaatsvindt. Zorg dat BZ centraal inzicht heeft welke ICT-diensten bij welke leverancier worden afgenomen en in hoeverre aan de gemaakte afspraken wordt voldaan door zowel de leverancier als BZ.
  - Acteer rolvast door SSC-ICT en andere dienstverleners als een voorspelbare partner te bevragen en ad hoc sturing te voorkomen. Realiseer binnen het ICT-domein een heldere taakafbakening, inclusief verdeling van verantwoordelijkheden om centrale

coördinatie en prioriteitsstelling te realiseren als het gaat om verzoeken aan dienstverleners.

- Verbeter de uitvoering van de interne beveiligingsprocessen:
  - Zorg voor effectieve naleving van de vereisten uit de BZ-beveiligingsbaseline en een gestructureerd informatiebeveiligingsproces binnen BZ. Verbeter ook de afhandeling van beveiligingsincidenten, waarbij altijd de grondoorzaak wordt onderzocht.
  - Bewaak naleving van de regels vanuit het accreditatiebeleid. Neem in de beoordeling van systemen die gerubriceerde informatie verwerken minimaal de relevante (technische) informatiebeveiligingskaders mee.

3. Realiseer vanuit BZK een rijksbrede aanpak beveiliging tegen statelijke actoren

Gezien de urgentie om beveiliging tegen statelijke actoren en georganiseerde criminaliteit (BBN3) effectief in te vullen, adviseren we BZK met hoge prioriteit een rijksbrede aanpak te realiseren. Maak duidelijk dat dit onderwerp ‘chefsache’ is door het opdrachtgeverschap in het Secretarissen-Generaal Overleg (SGO) te beleggen. We adviseren een rijksbrede aanpak bestaande uit twee onderdelen:

- Realiseer onder aansturing van CIO-rijk binnen zes maanden een uitwerking voor een rijksbreed kader voor de beveiliging tegen statelijke actoren:
  - Mobiliseer specialistische kennis vanuit tenminste de AIVD, MIVD, NCSC, BZ en andere ministeries.
  - Hanteer als uitgangspunt de informatiebeveiligingsnorm ISO27001 en laat het rijksbrede kader daarop aanvullend zijn. Dit is in lijn met de BIO die naar aanleiding van de Europese NIS2-richtlijn (Network and Information Security Directive) wordt vernieuwd.
  - Neem in het kader richtlijnen op voor het risicoanalyseproces ten aanzien van de wijze van selectie van beveiligingsmaatregelen (conform het risicobeoordeling en -behandelingsproces in de ISO27001). Zorg dat in dit risicoanalyseproces de specifieke karakteristieken en technieken van de modus operandi van statelijke actoren en criminele organisaties worden meegewogen, zoals het gebruik van wereldwijde interceptie.
  - Werk een selectie van toepasbare beveiligingsmaatregelen uit. Maak hierbij gebruik van bestaande goede voorbeelden vanuit ministeries, zoals specifieke cryptografische oplossingen, datadiodes voor veilige verbinding met minder veilige netwerken en virtualisatie-oplossingen. Zorg dat deze selectie actueel blijft.
  - Neem detectieregels op om mogelijke inbreuken tijdig te signaleren. Hanteer hiervoor het *Assume Breach*-principe. Dit gaat ervanuit dat niet voorkomen kan worden dat een aanvaller er uiteindelijk in slaagt om een systeem te compromitteren.
- Realiseer stapsgewijs BBN3 ICT-dienstverlening voor rijksbreed gebruik:
  - Bepaal welke overheidspartij het meest geschikt is om BBN3 ICT-dienstverlening te ontwikkelen op basis van het bovenstaande rijksbrede kader.
  - Faciliteer vanuit die overheidspartij de rijksbrede beschikbaarheid van tenminste een BBN3-werkplek. Een goede samenwerking tussen de verschillende ICT-dienstverleners en de datacentra binnen de rijksdienst is daarbij cruciaal.

4. Evalueer na twee jaar gezamenlijk de opvolging van de adviezen

Wij verwachten dat de opvolging van bovenstaande adviezen twee jaar in beslag zal nemen. Wij adviseren:

- Evalueer na twee jaar, of eerder indien opportuun, de opvolging van de adviezen en de effectiviteit van de getroffen maatregelen. Doe dat zowel bij BZ als SSC-ICT. Selecteer hiervoor een partij die onafhankelijk is ten opzichte van BZ en SSC-ICT.

- Bepaal op basis van de uitkomsten van de evaluatie eventuele vervolgstappen. Neem daarin mee hoe om te gaan met het uitgestelde vertrekbesluit. Werk een eventueel scenario voor een transitie dan pas uit, zodat de opbrengsten uit onze adviezen onder 2 (betere besturing BZ) en 3 (rijksbrede aanpak statelijke actoren) meegenomen kunnen worden in de uitwerking.

***

Wij danken alle geïnterviewden voor hun medewerking en openheid. Wij hopen dat we met dit advies een bijdrage kunnen leveren aan zowel het verbeteren van de ICT-dienstverlening bij BZ en SSC-ICT als aan het rijksbreed verbeteren van de weerbaarheid tegen statelijke actoren en criminele organisaties.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

Adri de Bruijn
Voorzitter

w.g.

Sander van Amerongen
Secretaris-directeur

Bijlage

Datum
3 februari 2025

Kenmerk
2025-0000122205

Informatie over programma Transitie ICT-dienstverlening

Nr.	Onderwerp	Toelichting
1.	Projectnaam	Transitie ICT-dienstverlening
2.	Opdrachtgever	Plaatsvervangend secretaris-generaal van het ministerie van Buitenlandse Zaken (BZ)
3.	Startdatum project	Nog niet formeel gestart
4.	Einddatum project	Nog niet bekend
5.	Type project	Transitie van de ICT-dienstverlening naar een andere dienstverlener
6.	Fase Project	Initiatiefase
7.	Totaal budget	Nog niet bekend
8.	Reeds uitgegeven per datum	Niet bekend
9.	Doelstelling	Ontvlechten en herbeleggen van (een nog te bepalen gedeelte van) de dienstverlening geleverd door SSC-ICT aan BZ
10.	Maatschappelijke/ beleidsdoelstelling	Niet gedefinieerd
11.	Meetbare baten	Geen meetbare baten gedefinieerd
12.	Huidige technologie/ architectuur	Grote diversiteit aan hardware en software
13.	Doeltechnologie/- architectuur	Nog niet bekend
14.	Omvang systeem	Niet bekend
15.	Aantal gebruikers	Circa 7600 werkplekgebruikers (ca. 4000 in Nederland en 3600 op buitenlandse posten)
16.	Belanghebbenden	• Medewerkers van BZ binnen en buiten Nederland • Bondgenoten en inlichtingen- en veiligheidsdiensten voor uitwisseling van informatie over geopolitieke ontwikkelingen en dreigingen • Afnemers van ICT-dienstverlening van SSC-ICT
17.	Aanbesteding voorzien	Nog niet bekend, afhankelijk van het te kiezen scenario

Informatie over het uitgevoerde onderzoek

Nr.	Onderwerp	Toelichting
1.	Type onderzoek	Project; conform artikel 7, lid 1 sub a2 Wet Adviescollege ICT- toetsing
2.	Aanmelddatum	22 augustus 2024
3.	Start onderzoek	29 augustus 2024
4.	Afronden onderzoek	5 december 2024
5.	Datum conceptadvies	19 december 2024
6.	Datum definitief advies	3 februari 2025
7.	Eerder onderzoek	Nee
8.	Onderzoeksmethode	Interviews en documentstudie