Auditrapport CIOT 2017

Concernaudit i.s.m. auditfuncties eenheden

Definitief

1.0

28 april 2020

Vertrouwelijk

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing
0.2	8 november 2018	Initiële versie
0.7	6 december 2018	Conceptversie t.b.v. review eenheidsauditoren
0.8	18 december 2018	Voorlopig concept
0.9	19 december 2018	Review coördinator CA verwerkt
1.0	28 april 2020	definitief

Distributie

Versie	Verzend datum	Afdeling / Functie
0.10	1 mei 2019	Lid Korpsleiding
0.11	13 mei 2019	PH CIOT
0.11	13 mei 2019	Politiechef Landelijke Eenheid
1.0	28 april 2020	Lid Korpsleiding

Inhoudsopgave

Documentinformatie 2

Inhoudsopgave 2

Aanleiding, doel en werkwijze audit 4
- Aanleiding 4
- Doel audit 4
- Werkwijze 4
- Leeswijzer 5

1. Verstrekking van telecomgegevens aan de politie 6

2. Belangrijkste conclusies en aanbevelingen 7
- 2.1. Landelijke procedure (bevragingen CIS) 7
- 2.2. Autoriseren 7
- 2.3. I&S 8
- 2.4. 112-centrale 8
- 2.5. Validatie steekproef 9

3. Bevindingen 10
- 3.1. Bevragingen CIS 10
  - 3.1.1. Procedure CIS-bevragingen 10
  - 3.1.2. Het gebruik van CIS (webcliënt CIOT) 10
  - 3.1.3. Het proces van bevragen 11
  - 3.1.4. Archivering 12
  - 3.1.5. Periodieke controle 12
  - 3.1.6. Toegangscontrole 12
- 3.2. Autorisaties 13
  - 3.2.1. Procedure autorisatieverlening 13
  - 3.2.2. Invulling taken beheerder 13
  - 3.2.3. Aanwijzing door de korpschef 14
  - 3.2.4. Opsporingsambtenaar of gecertificeerd BOA 14
  - 3.2.5. Deelname opleidingsdag CIOT 14
  - 3.2.6. Aanwijzing en rol landelijk coördinator 15
- 3.3. 112-centrale 15
  - 3.3.1. Toestemming minister afwijkende werkwijze 15
- 3.4. Validatie steekproef 16
  - 3.4.1. Uitvoering steekproef 16

Bijlage 1: toetskader steekproef 18

Aanleiding, doel en werkwijze audit

Aanleiding

De politie kan via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) klantgegevens van telecomaanbieders opvragen. De politie gebruikt deze informatie voor opsporingshandelingen en bij noodhulpverlening door de meldkamers.

Telecom- en internetbedrijven zijn wettelijk verplicht om persoonlijke gegevens die bij IP-adressen, telefoonnummers en e-mailadressen horen, beschikbaar te stellen aan het CIOT. Namens de minister van Justitie en Veiligheid zorgt het CIOT ervoor dat deze informatie, op verzoek, aan de politie verstrekt wordt. Hiertoe beheert het CIOT een geautomatiseerd informatiesysteem (CIS) voor telefoon- en internetgegevens.
Regels voor de verstrekking van gegevens van aanbieders van openbare telecommunicatienetwerken en –diensten met het oog op het strafvorderlijk onderzoek van telecommunicatie zijn vastgelegd in het Besluit verstrekking gegevens telecommunicatie.

In artikel 8 van dit besluit is bepaald dat de minister van Justitie en Veiligheid jaarlijks een verslag opstelt van een audit naar de goede uitvoering van dit besluit door de aanbieders van openbare telecomdiensten, van openbare telecommunicatienetwerkdiensten, van openbare telecommunicatienetwerken, het informatiepunt, de arrondissementsparketten en de politie, of andere opsporingsdiensten.
Daarbij worden tenminste de volgende onderwerpen behandeld:

a) de werking van het systeem;
b) de kwaliteit van de verstrekking van gegevens;
c) de bevraging van gegevens.

Voor de politie geldt dat de jaarlijkse audit naar de vaststelling van de goede uitvoering van het Besluit sinds 2013 onder verantwoordelijkheid van de korpschef van de politie valt. De korpschef heeft hiervoor de afdeling Concernaudit opdracht gegeven tot het uitvoeren van een politiebrede audit over het kalenderjaar 2017. Concernaudit heeft deze audit in samenwerking met de auditfuncties binnen de eenheden van de politie uitgevoerd.

Doel audit

Het doel van de audit is inzicht te geven in welke mate de politie voldoet aan de regels en afspraken gesteld aan de uitvoering van de bevraging van klantgegevens van telecom- en internetbedrijven via het CIOT. De periode van onderzoek is 2017.
Deze regels en afspraken zijn vastgelegd in:

- Het besluit verstrekking gegevens telecommunicatie, gewijzigd 01-01-2013;
- Het Service Level Agreement (SLA) tussen CIOT en de politie, versie 2.7;
- Het Dossier Afspraken en Procedures (DAP) tussen CIOT en de politie, versie 2.7.

Werkwijze

De audit is uitgevoerd door Concernaudit in samenwerking met auditoren uit de auditfuncties binnen de eenheden van de politie. Het gehanteerde toetsingskader is vastgesteld aan de hand van de regels en afspraken zoals vastgelegd in het besluit verstrekking gegevens telecommunicatie, het SLA en het DAP. Voor de uitvoering van de audit is gebruik gemaakt van interviews en documentenonderzoek. Ter validatie is aanvullend een steekproef uitgevoerd op de CIS-bevragingen in 2017, naar de naleving van bovengenoemde regels en afspraken.

Leeswijzer

Hoofdstuk 1 geeft een toelichting op en een korte indruk van het proces van verstrekking van de telecomgegevens binnen de politie.
Hoofdstuk 2 geeft kort de belangrijkste conclusies en aanbevelingen weer.
Hoofdstuk 3 geeft een volledig overzicht van de bevindingen.

1. Verstrekking van telecomgegevens aan de politie

De politie kan via het CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) actuele klantgegevens opvragen van telecomaanbieders. De politie is bevoegd deze informatie op te vragen in het kader van met name opsporingshandelingen. Het CIOT stelt deze gegevens beschikbaar via het CIOT Informatie Systeem (CIS). Toegang tot het CIS wordt door het CIOT verleend aan hiervoor geautoriseerde medewerkers (CIS-bevragers), via hiertoe door CIOT geautoriseerde werkplekken.

Een CIS-bevrager voert aan de hand van een verzoek van een opsporingsbevoegde of naar aanleiding van acute noodhulp de bevraging in het CIS in en verstrekt vervolgens het ontvangen antwoord aan de aanvrager.

Regels en afspraken over deze verstrekking van telecomgegevens zijn vastgelegd in:
- het Besluit verstrekking gegevens telecommunicatie, gewijzigd 01-01-2013;
- het Service Level Agreement (SLA) tussen CIOT en de politie, versie 2.7;
- het Dossier Afspraken en Procedures (DAP) tussen CIOT en de politie, versie 2.7.

De CIS-bevragingen voor de regionale eenheden worden uitgevoerd binnen Gemeenschappelijke BOB-kamers (GBK) per eenheid. Bij de Landelijke Eenheid worden de reguliere bevragingen uitgevoerd bij de afdeling Operationele Informatieverwerking (OIV). De afdeling Interceptie en Sensing (I&S) van de Landelijke Eenheid verzorgt de spoedbevragingen buiten kantoortijden en de no-hit doorbevragingen. Ook is de afdeling I&S het uitwijkpunt bij landelijke calamiteiten.
Deze CIS-bevragingen vinden hun basis in het wetboek van strafvordering (WvSv).

De politie maakt gebruik van terminals die specifiek zijn geautoriseerd voor het doen van CIS-bevragingen door het CIOT. De ruimte waarin deze terminals zijn geplaatst, is geclassificeerd als zijnde een kritische ruimte en dient alleen toegankelijk te zijn voor aangewezen bevoegd personeel.

Het CIOT beheert tevens de systeembevoegdheden (autorisaties) in het CIS.
Elke eenheid heeft naast CIS-bevragers ook maximaal twee beheerders. Een beheerder voert onder meer het beheer over de CIS-bevragers en ziet toe op de autorisaties van deze CIS-bevragers.
De beheerder verzorgt de aanmelding en afmelding van autorisaties van CIS-bevragers aan het CIOT, de landelijk coördinator doet dit voor de autorisaties van beheerders.

CIS-bevragers en beheerders dienen ten minste te voldoen aan de volgende criteria:
- aangewezen door of namens de korpschef;
- opsporingsambtenaar of gecertificeerd BOA;
- deelname opleidingsdag (CIS-bevrager/beheerder) bij het CIOT.

Daarnaast voert de 112-centrale ten behoeve van de meldkamers van de eenheden en de 112-centrale zelf ook CIS-bevragingen uit. Deze bevragingen betreffen situaties waarin sprake is van noodhulp of dusdanig misbruik van het 112-nummer dat de bereikbaarheid van de 112-centrale of de meldkamers in gevaar komt (bijvoorbeeld de zogenoemde ‘broekzakbellers’).

2. Belangrijkste conclusies en aanbevelingen

We constateren dat op verschillende punten uit de audit 2016 acties zijn ondernomen, maar dat een deel van deze acties ten tijde van de audit 2017 nog niet was geëffectueerd. Een groot deel van de bevindingen uit de audit 2016 is derhalve in deze audit weer geconstateerd. In onderstaande paragrafen geven we de belangrijkste conclusies en aanbevelingen weer.

I&S is verantwoordelijk voor het doen van spoedbevragingen buiten kantoortijden, doorbevragingen rechtstreeks bij de providers na een no-hit en het uitvoeren van bevragingen rechtstreeks bij providers bij calamiteiten (CIS systeem niet beschikbaar). Voor het bevragen rechtstreeks bij providers maakt I&S gebruik van het WMS systeem. Door haar specifieke werkzaamheden wijkt I&S af van de procedure CIOT. Om deze reden geven we de bevindingen inzake I&S separaat weer.

2.1. Landelijke procedure (bevragingen CIS)

We constateren dat de beschrijving van de landelijke procedure op een aantal punten aanscherping behoeft. Dit is reeds in de audit 2016 geconstateerd. We noemen hier met name de toetsing van de CIS-bevrager op de aanvraag, waaronder de controle op de opsporingsbevoegdheid van de aanvrager.
Er is nog onduidelijkheid over de wijze waarop bevragingen dienen plaats te vinden van telecomgegevens op een bepaalde datum of tijd in het verleden (de zogenoemde datum-tijdbevragingen), internationale rechtshulpverzoeken en embargo-onderzoeken. Tevens constateren we dat incidenteel rechtstreeks contact wordt opgenomen met een provider na een no-hit en dat bevragingen worden uitgevoerd in het kader van (terreur)oefeningen.

Op basis van de registratie van geautoriseerde werkstations (IP-adressen) van het Informatiepunt Bijzondere Opsporingsonderzoeken (IBO) laat de inventarisatie zien dat drie geautoriseerde werkstations zich bevinden buiten de aangewezen ruimten. In acht gevallen is het nog niet mogelijk geweest de administratieve aansluiting vast te stellen.

Aanbeveling
Op verzoek van de Portefeuillehouder voert de landelijk coördinator een actualisatie uit op de procedure CIOT. We bevelen aan om, voor zover dit nog niet is gebeurd, deze punten hierin mee te nemen. Daarnaast bevelen we aan om de registratie (bij de politie) van geautoriseerde werkstations te actualiseren en controleren met de registratie bij IBO, en het geautoriseerde werkstations buiten de aangewezen ruimten te deautoriseren.

2.2. Autoriseren

De landelijke Portefeuillehouder CIOT heeft het voornemen de procedure CIOT aan te passen mede naar aanleiding van de bevindingen hierover in de audit 2016. Een advies hiervoor is vanuit beleidsontwikkeling aangeboden aan de Portefeuillehouder CIOT. De herziende procedure beoogt onder meer ook de garantie te bieden dat bevragers en beheerders uitsluitend nog geautoriseerd kunnen worden voor het CIS-bevragingssysteem als zij (vooraf) voldoen aan de gestelde criteria. De procedure wordt ingericht op basis van de voorgestelde inrichting van de Interceptiedesk waar de CIS-bevragingen worden ondergebracht.

We constateren dat in het proces van autoriseren op een aantal punten nog niet wordt voldaan aan de regelgeving. De volgende bevindingen zijn geconstateerd:
- De voorgeschreven aanwijzing door de korpschef gebeurt per half jaar achteraf in plaats van vooraf.
- Bij de aanmelding van beheerders bij het CIOT wordt niet de voorgeschreven aanwijzing van de korpschef bijgevoegd. Deze aanwijzing gebeurt, zoals aangegeven, achteraf.

- De geldigheid van BOA certificering van bevragers en beheerders wordt niet structureel bij alle eenheden gecontroleerd. Hiervoor zijn geen landelijke afspraken of richtlijnen opgesteld.
- Er ontbreekt (historisch) inzicht in de deelname aan de verplichte opleidingsdagen door CIS-bevragers en beheerders. Sinds 2017 geeft CIOT (opleidings-)certificaten uit na deelname aan de opleidingsdag. De beheerder en de landelijk coördinator kunnen hiermee toetsen of voldaan wordt aan de opleidingseis voordat zij CIS-bevragers en beheerders aanmelden bij het CIOT. Aan deze toets wordt nog niet voldoende invulling gegeven.
- Het is niet duidelijk wie formeel nieuwe beheerders zou moeten benoemen. In de praktijk meldt de tweede beheerder de nieuwe beheerder aan bij de landelijk coördinator.
- De rol van de landelijk coördinator (taken en bevoegdheden) is (nog) niet formeel vastgesteld en de landelijk coördinator wordt ook (nog) niet formeel aangewezen. In de praktijk vervult de landelijk coördinator een belangrijke rol naar het CIOT, als aanspreekpunt, lid klankbordoverleg, aanmelding beheerders, etc.

Aanbeveling:
Op dit moment wordt gewerkt aan een nieuwe procedure waarbij de geconstateerde bevindingen reeds worden meegenomen. Gezien de afhankelijkheden van de inrichting van de Interceptiedesk adviseren we om hier prioriteit aan te geven. Indien de inrichting van de interceptiedesk meer tijd vergt, adviseren we vooruitlopend hierop tussentijdse maatregelen te treffen.

2.3. I&S

Door haar specifieke werkzaamheden wijkt I&S af van de werkwijze van andere eenheden. Om deze reden geven we de bevindingen inzake I&S separaat weer.

We constateren dat afspraken omtrent onderstaande werkwijzen niet zijn vastgelegd in de procedure CIOT:

- De procedure spoedbevragingen en de procedure doorbevragingen bij providers na een no-hit zijn niet nader beschreven in de procedure CIOT.
- De beheerder I&S heeft geen toegang tot de afdeling I&S vanwege het vertrouwelijke karakter van de werkzaamheden. Om deze reden wordt een deel van de rol van de beheerder uitgevoerd door andere functionarissen binnen I&S.
- Daarnaast voert de afdeling I&S geen periodieke steekproef uit.

I&S voert buiten kantoortijden voor Bijzondere Opsporingsdiensten (BOD's) spoedbevragingen uit. Een schriftelijke vastlegging van deze afspraken is tijdens de audit niet aangetroffen.
Daarnaast is voor het uitvoeren van bevragingen bij I&S de server geautoriseerd in plaats van de betreffende werkstations. Hiervan zijn geen vastgelegde afspraken aangetroffen.

Aanbeveling:
We adviseren ook de werkwijze van I&S vast te stellen en op te nemen in de procedure CIOT. Daarnaast adviseren we in overleg met het IBO van het CIOT afspraken te maken en vast te leggen omtrent het uitvoeren van spoedbevragingen ten behoeve van andere BOD's en omtrent het autoriseren van de server.

2.4. 112-centrale

De minister heeft in een schrijven van 14 november 2018 geconstateerd dat de 112-meldkamer in uitzonderlijke gevallen CIS-bevragingen uitvoert ten behoeve van noodhulp, terwijl hiervoor de wettelijke grondslag ontbreekt. De reden dat het CIOT voor noodhulpdoeleinden wordt bevraagd, is gelegen in het feit dat telecomaanbieders weliswaar wettelijk verplicht zijn om de NAWP gegevens van hun klanten aan de landelijke 112 meldkamer aan te leveren conform artikel 11.10 lid 3 TW, maar dat de directe

aanlevering soms nog op technische problemen stuit. In de praktijk zijn de NAWP gegevens direct na het beëindigen van het gesprek niet meer zichtbaar.

Naar verwachting wordt in april 2019 een nieuw 112 platform opgeleverd, waarin de directe aanlevering van NAWP gegevens vanuit de telecomaanbieders technisch is geregeld.
Dit overwegende, heeft de minister toestemming verleend om de bestaande werkwijze, dat de landelijke 112 meldkamer in uitzonderingsgevallen voor het verlenen van snelle en adequate noodhulp, voor de duur van een halfjaar vanaf 14 november 2018 of zoveel eerder tot aan de oplevering van het nieuwe 112 platform, voort te zetten.

Bevinding:
Aanvragen in het kader van noodhulp en misbruik hebben een ander karakter dan opsporing. De voorwaarden voor het kunnen gebruiken van het CIS conform het Besluit, het SLA en de DAP verhouden zich onvoldoende tot het spoedeisende karakter van de noodhulp.
In de praktijk zien we dat de 112-meldkamer op een aantal punten afwijkend van de regelgeving handelt.

In een aantal gevallen zijn hiervoor door de 112 meldkamer aanvullende maatregelen genomen.
De minister stemt toe tijdelijk de bestaande werkwijze voort te zetten. We hebben echter vastgesteld dat deze werkwijze, de (afwijkende) procedure en aanvullende maatregelen, nog niet zijn vastgelegd.

Daarnaast is het onduidelijk of deze toestemming ook de mogelijkheid biedt voor medewerkers van de ambulancedienst en brandweer van de regionale meldkamers om CIS-bevragingen te laten uitvoeren. In de steekproef is 1 post aangetroffen waarbij de aanvraag voor een CIS bevraging in het kader van noodhulp van een medewerker van de ambulancedienst van de regionale meldkamer afkomstig is.

Aanbeveling:
We adviseren het 112 platform zo spoedig mogelijk te implementeren. Daarnaast dient vastgesteld te worden of medewerkers van de ambulancedienst en brandweer van de regionale meldkamers ook CIS-bevragingen mogen laten uitvoeren.

2.5. Validatie steekproef

De resultaten van de steekproef van ruim 200 CIS-bevragingen bevestigen de hierboven genoemde verbeterpunten.

3. Bevindingen

Op basis van de uitgevoerde audit komen we tot de onderstaande bevindingen. De bevindingen hebben betrekking op de onderdelen bevragingen CIS (3.1) en de autorisaties (3.2). De bevindingen bij de 112-centrale staan apart weergegeven (3.3), dit gezien het specifieke karakter.
Ter validatie van de onderzoeksresultaten is een steekproef uitgevoerd op de CIS-bevragingen in 2017, de bevindingen hierover staan in paragraaf 3.4.

3.1. Bevragingen CIS

Telecom- en internetbedrijven zijn wettelijk verplicht om persoonlijke gegevens die bij IP-adressen, telefoonnummers en e-mailadressen horen, beschikbaar te stellen aan het CIOT. Namens de minister van Justitie en Veiligheid zorgt het CIOT ervoor dat deze informatie, op verzoek, aan de politie verstrekt wordt. Hiertoe beheert het CIOT een geautomatiseerd informatiesysteem (CIS) voor telefoon- en internetgegevens. In de volgende sub paragrafen worden de bevindingen met betrekking tot het bevragen van het CIS weergegeven.

3.1.1. Procedure CIS-bevragingen

De politie maakt gebruik van een landelijke procedure vastgelegd in de ‘Procedure CIOT bevragingen’. Deze procedure CIOT bevragingen is medio 2016 geactualiseerd en op 1 september 2016 verspreid naar onder meer de politiechefs van de eenheden en hoofden Gemeenschappelijke BOB-kamer (GBK).

Bevinding:
Uit interviews blijkt dat de procedure CIOT bevragingen over het algemeen bekend is. Bij I&S wordt gebruik gemaakt van een eigen procedure voor spoedbevragingen en doorbevragingen bij providers na no-hits of bij calamiteiten, indien het CIS systeem niet beschikbaar is.

3.1.2. Het gebruik van CIS (webcliënt CIOT)

Voor het opvragen van klantgegevens bij de telecomaanbieders wordt alleen het CIS (webcliënt CIOT) gebruikt. Uitzonderingen hierop zijn:
- doorbevraging na no-hit (bevraging geeft aan geen resultaat gevonden);
- bevragingen bij calamiteiten.

Doorbevragingen na no-hit en bevragingen bij calamiteiten worden alleen uitgevoerd door CIS-bevragers van I&S. Hierbij wordt door I&S via een beveiligde lijn de informatie bij providers opgevraagd. Daarbij wordt gebruik gemaakt van het systeem WMS.

Bevindingen:
Incidenteel geven CIS-bevragers aan dat zij na een no-hit zelf contact zoeken met de betreffende telecomaanbieder. Deze CIS-bevragers geven hierbij aan dat ze niet bekend waren met het proces doorbevraging op basis van no-hit (bevraging geeft aan geen resultaat gevonden) via I&S.

Meestal betreffen bevragingen actuele gegevens. Het kan echter voorkomen (na een no-hit) dat een bevraging wordt gedaan naar historische klantgegevens (de zogenoemde datum-tijd bevragingen) bij een telecomaanbieder. Het CIS geeft alleen geautomatiseerd toegang tot actuele gegevens van de telecomaanbieders en kan hiervoor dus niet worden gebruikt. Voor het doen van de zogenoemde datum-tijd bevragingen na een no-hit zijn de kaders en procedure nog niet vastgesteld. Uit interviews blijkt dat dit in de praktijk bij enkele eenheden verschillend wordt ingevuld, ofwel CIS-bevragers in eenheden hebben zelf contact met de telecomaanbieder ofwel I&S voert de bevraging in via WMS.

In de steekproef is geconstateerd dat één bevraging is uitgevoerd in het kader van een terreuroefening, Hierbij zijn bevragingen uitgevoerd op telefoonnummers behorende bij prepaid telefoons die de politie

heeft aangeschaft voor deze oefening. Tevens is aangegeven dat goedkeuring is verkregen van de OvJ. De regelgeving voorziet niet in een dergelijke bevraging

3.1.3. Het proces van bevragen

Aanvragen voor bevragingen worden door de OvJ of opsporingsbevoegde per mail naar het GBK verstuurd. De CIS-bevragers toetsen de aanvraag op de naleving van de voorschriften. In de landelijke procedure zijn de criteria voor deze toetsing beschreven.
Er bestaat ook de mogelijkheid dat bij lopende taps of historische (telefoon) verkeersgegevens de hierop betrekking hebbende telefoonnummers geautomatiseerd worden verzameld en worden aangeboden aan het GBK. Hiertoe is het wel noodzakelijk dat door een OvJ een vordering is afgegeven. Deze machtiging wordt in het informatiesysteem SUMM-IT vastgelegd. Dit systeem genereert, indien deze machtiging is aangegeven, een automatische aanvraag bij het GBK in de vorm van een txt-bestand. De toets van de CIS-bevrager op de aanvraag richt zich bij deze aanvragen op een controle op de aanwezigheid van een parketnummer en de onderzoeksnaam.
Er kan sprake zijn van een spoedbevraging. Hierbij dient sprake te zijn van één van de genoemde spoedcriteria. Bij een spoedbevraging kan via de mail (vast format) een bevraging worden aangevraagd en dient het proces-verbaal (PV) binnen 3x24 uur te worden aangeleverd.
Het proces van CIS-bevragen wordt geautomatiseerd ondersteund door Poli-OM. De landelijke eenheid waaronder ook de 112-centrale en I&S, maakt geen gebruik van Poli-OM.
In de audit 2016 is vastgesteld dat de (schriftelijke) procedure op een aantal punten nog aanscherping behoeft. Hiertoe was al een aanzet gemaakt, maar daadwerkelijke aanpassing van de formele procedure heeft nog niet heeft plaatsgevonden. We benoemen onderstaand deze punten die al in de audit 2016 zijn benoemd.

Bevindingen:
We hebben vastgesteld dat mede door het gebruik van formats, de landelijke procedure en het gebruik van Poli-OM landelijke eenduidigheid bestaat. Dit betreft aanvragen, afhandeling en archivering in Poli-OM van en de toetsing op CIS-bevragingen

Uit interviews bij de eenheden komt naar voren dat de wijze waarop de toetsen zijn beschreven op punten nog aanscherping behoeft. Er staat bijvoorbeeld wel aangegeven wat het onderwerp van een toets is, maar wat er precies moet worden getoetst kan verschillend worden geïnterpreteerd. Nieuwe medewerkers worden, na de opleiding, ingewerkt door ervaren krachten. Hierdoor wordt het risico in de praktijk deels opgevangen.
Eén van de toetsen die de CIS-bevrager uitvoert op de aangeleverde aanvraag, is de toets op de opsporingsbevoegdheid van de aanvrager. Uit interviews blijkt dat deze toets wordt uitgevoerd aan de hand van de functiebenaming van de aanvrager in het PV. Met de vorming van de politie zijn functiebenamingen gewijzigd, waardoor de opsporingsbevoegdheid niet in alle gevallen meer uit de functienaam te herleiden is.

Tevens is uit interviews en uit de controle op de steekproef gebleken dat er naast de in de procedure aangegeven soorten aanvragen in de praktijk ook aanvragen binnenkomen op basis van een internationaal rechtshulpverzoek en embargo-onderzoeken. Eenheden hanteren hiervoor verschillende werkwijzen. Er ligt een voorstel voor een procedure voor embargo en internationaal rechtshulpverzoek bij de landelijke coördinator. Dit voorstel dient nog te worden vastgesteld en te worden opgenomen in de procedure CIOT. Vooruitlopend hierop wordt de werkwijze wel besproken in de beheerders- en bevragersopleiding CIOT.

I&S voert na kantoortijden spoedbevragingen uit op verzoek van een aantal andere Bijzondere Opsporingsdiensten (BOD's), zoals de Fiscale Inlichtingen- en Opsporingsdiensten, de Algemene Inspectiedienst en de Rijksrecherche. In interviews is aangegeven dat hier in het verleden afspraken over zijn gemaakt. Een schriftelijke vastlegging van deze afspraken is tijdens de audit niet aangetroffen.

Bij spoedbevragingen dienen de aanvullende stukken binnen 3x24 uur te worden aangeleverd. Het systeem Poli-Om voorziet hierin door de posten als ‘openstaand’ zichtbaar te houden en automatisch te reclameren bij de aanvrager. Uit interviews en uit de steekproef is gebleken dat het voorkomt dat de termijn van 3x24 uur wordt overschreden, de overschrijding beperkt zich tot maximaal één week.

3.1.4. Archivering

Zowel de aanvraag als het ontvangen resultaat worden gearchiveerd. Het systeem Poli-OM ondersteunt hierin. De procedure geeft een archiveringstermijn van zeven jaar aan.

Bevindingen:
De termijn van zeven jaar is niet verder onderbouwd. In de praktijk worden er verschillende termijnen gehanteerd, waarbij we binnen de eenheden geen kortere termijn dan drie jaar zijn tegengekomen.

In de praktijk komt het voor dat er bevragingen worden gedaan ten behoeve van embargo-onderzoeken. In dit geval mag er geen archivering bij de GBK plaatsvinden. Ook kan de officier van justitie een bevel geven tot verwijdering van specifieke politiegegevens. Zowel voor de verwijdering op verzoek van de officier van justitie als voor het embargo-onderzoek is niet vastgesteld wat minimaal gearchiveerd moet worden om de bevraging achteraf te kunnen verantwoorden (zoals bij een periodieke controle of audit). Aan deze aanbeveling is in 2017 geen opvolging gegeven. Dit punt wordt momenteel door de landelijk coördinator CIOT opgepakt en in de bevragers- en beheerdersopleiding besproken.

3.1.5. Periodieke controle

Beheerders binnen de eenheden controleren conform de procedure CIOT eens per drie maanden minimaal twintig bevragingen op een juiste verwerking en archivering. Deze controle, inclusief de nazorg op de bevindingen, wordt vastgelegd.

Bevindingen:
We stellen vast dat alle eenheden deze controle in 2017 hebben uitgevoerd met uitzondering van één eenheid. Deze controle is echter per direct weer opgepakt. Daarnaast voert de afdeling I&S geen periodieke steekproef uit. I&S voert alleen spoedbevragingen en bevragingen bij calamiteiten uit ten behoeve van andere eenheden. Deze bevragingen worden in de betreffende eenheid afgehandeld en gearchiveerd. Voor I&S is het wel noodzakelijk vast te stellen dat elke bevraging in CC naar de desbetreffende eenheid is gestuurd.

3.1.6. Toegangscontrole

De ruimte waarin de voor CIS geautoriseerde werkplekken zijn geplaatst, is alleen toegankelijk voor aangewezen bevoegd personeel en is geclassificeerd als zijnde een kritische ruimte.

Bevindingen:
CIS- werkplekken binnen de GBK’s bevinden zich in afgesloten ruimtes die alleen toegankelijk zijn voor geautoriseerd personeel. In een aantal gevallen is het GBK geplaatst binnen het OM, rechtbank of Paleis van Justitie en valt daartoe onder de daar geldende regelgeving.

Uit interview en waarneming bij verschillende GBK’s constateren we dat CIS-bevragers en beheerders in de praktijk zorgvuldig en bewust omgaan met het fysiek toegang verlenen tot de ruimte en de informatie in het CIS-systeem, door bijvoorbeeld een goede uitlogdiscipline en het afschermen van het beeldscherm voor onbevoegden.

De administratie van IBO geeft aan dat er 78 werkstations (IP-adressen) bij de politie zijn geautoriseerd voor CIOT-bevragingen. We hebben vastgesteld dat hiervan 67 werkstations zich in de aangewezen ruimten bevinden.
In drie gevallen bevindt het werkstation zich in een andere ruimte. 1 IP-adres betreft een server (I&S) in plaats van een werkstation. De hieraan verbonden werkstations bevinden zich in de beveiligde ruimte van I&S,
In acht gevallen is het nog niet mogelijk geweest de administratieve aansluiting vast te stellen.

3.2. Autorisaties

Een bevraging moet worden uitgevoerd door een CIS-bevrager, een hiertoe geautoriseerd ambtenaar.

Per eenheid zijn tevens maximaal twee beheerders aangewezen. Taken en verantwoordelijkheden van deze beheerders zijn (in het kader van autorisaties):
- het voeren van het beheer over de CIS-bevragers van de betreffende eenheid;
- aanvragen en opheffen van gebruikersaccounts;
- aanvragen van wachtwoord resets;
- het uitreiken van de gebruikersaccounts.

CIS-bevragers en beheerders dienen ten minste te voldoen aan de volgende criteria:
- aangewezen door de korpschef;
- opsporingsambtenaar of BOA;
- deelname opleidingsdag (CIS-bevrager/beheerder) CIOT.

3.2.1. Procedure autorisatieverlening

De landelijke Portefeuillehouder CIOT heeft het voornemen de procedure CIOT aan te passen mede naar aanleiding van de bevindingen hierover in de audit 2016. Een advies hiervoor is vanuit beleidsontwikkeling aangeboden aan de Portefeuillehouder CIOT. De herziende procedure beoogt onder meer ook de garantie te bieden dat bevragers en beheerders uitsluitend nog geautoriseerd kunnen worden voor het CIS-bevragingssysteem als zij (vooraf) voldoen aan de gestelde criteria.

Bevinding:
We stellen vast dat in de procedure CIOT-bevragingen het proces van autorisatieverlening is opgenomen. Hierin wordt aangegeven dat het aanvragen van een account, het opheffen van een account en het aanvragen van een wachtwoordreset voor een CIS-bevrager door de beheerder via het standaardformulier wordt gemeld aan de servicedesk CIOT. Het aanvragen, opheffen en aanvragen van een wachtwoordreset voor de beheerders wordt gedaan door de landelijk coördinator CIOT. Maandelijks wordt vanuit het CIOT een lijst met de actuele autorisaties verzonden naar de beheerders van de eenheid. Uit interviews en documentenonderzoek is geconstateerd dat deze lijst structureel door de beheerders wordt gecontroleerd en afwijkingen worden teruggekoppeld aan het CIOT. Tevens hebben we op basis van interviews vastgesteld dat bij het verlaten van de dienst of andere werkzaamheden de beheerder de betreffende bevrager op inactief zet in het CIS webcliënt. Hierbij zijn twee afwijkingen aangegeven. Twee accounts van bevragers niet zijn gedeactiveerd. Dit betrof een account bij langdurige ziekte en een account bij een (tijdelijke) andere plaatsing.

3.2.2. Invulling taken beheerder

Taken en verantwoordelijkheden van de lokale beheerder zijn het beheer voeren over de CIOT-gebruikers, het aanvragen van gebruikersaccounts en het uitreiken van certificaten aan de gebruikers van het CIOT-informatiesysteem voor de organisatie/eenheid.

Bevinding:
Uit interviews blijkt dat de taken en verantwoordelijkheden van beheerders worden uitgevoerd conform procedure CIOT met uitzondering van I&S. De CIS beheerder I&S heeft zelf geen toegang tot de afdeling I&S vanwege het vertrouwelijke karakter van de werkzaamheden. Om deze reden wordt een deel van de rol van de beheerder uitgevoerd door andere functionarissen binnen I&S. Zo verzorgt de systeembeheerder van I&S de uitgifte van nieuwe wachtwoorden. Afspraken over deze afwijkende werkwijze zijn niet vastgelegd.

3.2.3. Aanwijzing door de korpschef
CIS-bevragers en beheerders dienen te zijn aangewezen door of namens de korpschef.

Bevindingen:
Wij stellen vast dat de korpschef de aanwijzing van alle actieve gebruikers (CIS-bevragers en beheerders) ongeveer twee maal per jaar bekrachtigt via een lijst met alle actieve gebruikers. Deze bekrachtiging van beheerders en CIS-bevragers vindt hiermee niet vooraf plaats maar maximaal zes maanden na het afgeven van de systeemautorisatie.

De aanvraag voor een CIS systeemautorisatie wordt bij bevragers altijd geaccordeerd door de beheerder. In het geval van een systeemautorisatie voor een beheerder dient de landelijk coördinator te accorderen. Uit de interviews blijkt dat een vertrekkende beheerder of de tweede beheerder van een eenheid de aanmelding verzorgt van een nieuwe beheerder aan de landelijk coördinator CIOT. Het is niet duidelijk wie bevoegd is nieuwe beheerders te benoemen.

Bij de aanmelding van nieuwe beheerders dient goedkeuring van de korpschef als bijlage bij het aanmeldingsformulier (formulier aanvraag CIS account lokale beheerder) gevoegd te worden en verstuurd te worden aan de servicedesk CIOT. De landelijk coördinator keurt de aanmelding op dit formulier goed. Er wordt echter geen schriftelijke aanwijzing korpschef bijgevoegd.

3.2.4. Opsporingsambtenaar of gecertificeerd BOA
Elke actieve gebruiker van het CIS (beheerder en bevrager) dient ten tijde van zijn/haar bevragingen opsporingsbevoegd te zijn. Een beheerder of bevrager is opsporingsbevoegd als hij/zij algemeen opsporingsambtenaar of gecertificeerd BOA is.

Bevindingen:
Uit interviews blijkt dat de afloop van de BOA certificering niet structureel bij alle eenheden wordt gecontroleerd om tijdig de hercertificering van de BOA te kunnen initiëren.

Aanvullend is van alle bevragingen in 2017 vastgesteld of de bevragingen zijn uitgevoerd door een opsporingsbevoegde bevrager. Hiervoor is de personeelsadministratie geraadpleegd. Daar waar dit onvoldoende duidelijkheid gaf, zijn hiervoor aanvullende documenten opgevraagd.
We stellen vast dat alle bevragingen zijn uitgevoerd door opsporingsbevoegde bevragers. Bij twee bevragers heeft de hercertificering voor de BOA wel voor de afloopdatum van de BOA plaatsgevonden maar zijn de medewerkers pas na de afloopdatum beëdigd als opsporingsambtenaar voor de nieuwe periode.

3.2.5. Deelname opleidingsdag CIOT
De lokale beheerders melden nieuwe CIS-bevragers bij CIOT aan voor deelname aan de opleidingsdag CIOT. De landelijk coördinator meldt de beheerders aan. De deelname aan de opleiding is een vereiste om geautoriseerd te worden voor CIS-bevragingen.

Bevinding:

In het verleden was er geen historisch inzicht in de deelname aan de opleidingsdagen. In de loop van 2017 is CIOT gestart met het uitreiken van opleidingscertificaten door CIOT na het afronden van de opleiding. Op basis hiervan kan worden vastgesteld dat een beheerder of bevrager de opleiding heeft doorlopen.

Uit interviews blijkt dat bevragers over het algemeen de opleidingsdag hebben doorlopen voor zij geautoriseerd worden voor CIS-bevragingen. In een enkel geval is aangegeven dat een bevrager reeds geautoriseerd was voor het doorlopen van de opleiding. Daarnaast geven vijf beheerders aan dat zij de beheerderscursus niet hebben gevolgd, maar wel als beheerder zijn geautoriseerd, hieronder bevindt zich één recent aangestelde beheerder.

3.2.6. Aanwijzing en rol landelijk coördinator

Binnen de politie is invulling gegeven aan de rol van landelijk coördinator. De landelijk coördinator is (in de praktijk) onder andere het eerste aanspreekpunt voor CIOT, verzorgt deze de aanmelding/reset wachtwoord/ opheffen CIS account van de lokale beheerders, is lid van het klankbordoverleg en het stuurgroepoverleg namens de politie, beheert en actualiseert de procedure en is docent van de opleiding CIOT.

Bevinding:
De rol van landelijk coördinator is niet opgenomen in wet- en regelgeving en is niet als rol formeel ingericht binnen de politie. Het mandaat van de landelijk coördinator is ook niet beschreven. Deze rol wordt nu vormgegeven door een beheerder van een eenheid, die dit landelijk oppakt naast zijn/haar beheerderstaken. Hoewel deze rol niet formeel is ingericht, en er geen afspraken over vastliggen, stellen we vast dat het IBO alleen aanvragen voor het autoriseren van beheerders accepteert als deze zijn geautoriseerd door de landelijk coördinator.

3.3. 112-centrale

De 112-centrale voert ten behoeve van de meldkamers van de eenheden en de 112-centrale tijdelijk zelf CIS-bevragingen uit. Bij deze bevragingen is er sprake van noodhulp of sprake van een dermate misbruik van het noodnummer waarbij de bereikbaarheid van de 112-centrale onder druk komt te staan.
Gezien het specifieke en tijdelijke karakter worden de bevindingen hierover separaat weergegeven.

3.3.1. Toestemming minister afwijkende werkwijze

De minister heeft in een schrijven van 14 november 2018 geconstateerd dat de 112-meldkamer in uitzonderlijke gevallen CIS-bevragingen uitvoert ten behoeve van noodhulp, terwijl hiervoor de wettelijke grondslag ontbreekt.
De reden dat het CIOT voor noodhulpdoeleinden wordt bevraagd, is gelegen in het feit dat telecomaanbieders weliswaar wettelijk verplicht zijn om de NAWP gegevens van hun klanten aan de landelijke 112 meldkamer aan te leveren conform artikel 11.10 lid 3 TW, maar dat de directe aanlevering soms nog op technische problemen stuit. Het CIOT systeem, waar elke 24 uur door alle telecomaanbieders de NAWP gegevens van klanten gekoppeld aan het telefoonnummer worden aangeleverd, biedt dan een uitwijk.
De politie mag ten behoeve van de noodhulp dus wel rechtmatig over de gegevens beschikken, maar daarvoor niet het CIOT systeem raadplegen.
Door de toegang tot het CIS is het mogelijk om toch de noodzakelijke gegevens te krijgen ten behoeve van noodhulp en het bovengenoemde misbruik van het 112-nummer.
Naar verwachting wordt in april 2019 een nieuw 112 platform opgeleverd, waarin de directe aanlevering van NAWP gegevens vanuit de telecomaanbieders technisch is geregeld.
Dit overwegende, heeft de minister toestemming verleend om de bestaande werkwijze, dat de landelijke 112 meldkamer in uitzonderingsgevallen voor het verlenen van snelle en adequate noodhulp, voor de duur van een halfjaar vanaf 14 november 2018 of zoveel eerder tot aan de oplevering van het nieuwe

112 platform, voort te zetten. Daarbij verzoekt de minister om bij te houden in hoeveel gevallen het CIOT systeem door de landelijke 112 meldkamer in het kader van noodhulp wordt bevraagd en de minister deze cijfers na dit halfjaar te overleggen.

Bevinding:
De centralist van de (112-)meldkamer krijgt in principe de adresgegevens mee met het inkomende gesprek, dit zijn de COIN1 gegevens. Alleen als de gegevens niet beschikbaar zijn of het gesprek is verbroken (waardoor de COIN gegevens niet meer zichtbaar zijn) en op terugbellen niet wordt gereageerd, is er noodzaak voor een CIOT bevraging.

Het Besluit verstrekking gegevens telecommunicatie, het SLA en het DAP richten zich met name op de aanvragen op basis van grondslagen van het Wetboek van Strafvordering. Aanvragen in het kader van noodhulp hebben een ander karakter dan opsporing. De voorwaarden voor het kunnen gebruiken van het CIS conform het Besluit, het SLA en de DAP verhouden zich onvoldoende tot het spoedeisende karakter van de noodhulp. In de praktijk zien we hierdoor dat op een aantal punten voor de noodhulp van het 112-nummer afwijkend van de regelgeving wordt gehandeld.
In een aantal gevallen zijn hiervoor door de 112 meldkamer aanvullende maatregelen genomen.
De minister stemt toe tijdelijk de bestaande werkwijze voort te zetten, we stellen vast dat deze werkwijze, de (afwijkende) procedure en aanvullende maatregelen, nog niet is vastgelegd.

Medewerkers van de regionale meldkamers kunnen in het kader van noodhulp een verzoek om een CIS-bevraging doen aan de CIS-bevrager van de 112-meldkamer. Uit interview blijkt dat naast politie, dit ook op verzoek van een medewerker van de ambulancedienst of brandweer zijn. Dit verzoek wordt dan voorzien van een aanvraag getekend door een opsporingsambtenaar. De toestemming van de minister geeft hier geen duidelijkheid over.

Uit de bevragingen in 2017 is een steekproef samengesteld van zestien posten. Hierbij is rekening gehouden met een spreiding over de verschillende accounts. Daarnaast zijn de drie posten geselecteerd met een afwijkende rechtsgrondslag. Deze posten zijn getoetst op een juiste behandeling.
We constateren dat er in één geval sprake is van een aanvraag van een (onbevoegde) medewerker van de ambulancedienst. In drie gevallen is abusievelijk de rechtsgrondslag WvSv 126 NA ingevoerd in het CIS in plaats van TW11.10.

- 1 x betreft dit feitelijk misbruik van het noodnummer.
- 2 x betreft dit feitelijk noodhulp.

3.4. Validatie steekproef

Ter validatie is aanvullend op basis van een steekproef een dossieronderzoek uitgevoerd naar de naleving van de genoemde regels en afspraken met betrekking tot verstrekking telecomgegevens. Voor de bepaling van de steekproef zijn posten geselecteerd over het kalenderjaar 2017.

3.4.1. Uitvoering steekproef

De politie heeft in 2017 ruim 140.000 bevragingen uitgevoerd in het CIS. Deze CIS-bevragingen zijn de basis geweest voor het bepalen van de steekproef van ruim 200 bevragingen. Ten behoeve van de audit 2016 is een uitgebreide steekproef uitgevoerd. De resultaten van deze steekproef lieten geen bijzondere afwijkingen zien. Dit jaar is gekozen om bij de steekproef het aantal geautomatiseerde posten vanuit SUMMIT te beperken. Daarnaast is de steekproef uitgevoerd met een focus op de risicovolle deelpopulaties binnen de uitgevoerde bevragingen. Voorbeelden van deelpopulaties:

- bevragingen door (in 2017) nieuwe beheerders;

[1] Noot notulist: COIN is een samenwerking van Nederlandse aanbieders van elektronische communicatiediensten en –netwerken. Ze beheren een database met alle actieve telefoonnummers in Nederland. Wanneer wordt gesproken over COIN gegevens worden de gegevens uit deze database bedoeld.

- bevragingen op incidenteel voorkomende rechtsgrondslagen
- bevragingen die meer dan 1000 vragen bevatten. (context: elke CIS-bevraging kan één of meerdere vragen bevatten)
- spoedbevragingen buiten kantoortijd.

De aanvragen behorende bij de bevragingen zijn onder meer getoetst op aanwezigheid van (mede afhankelijk van het soort bevraging):
- naam en handtekening bevoegde autoriteit;
- bevel/vordering OvJ;
- rechtsgrondslag en wetsartikel;
- dossierkenmerk (onderzoeksnummer).

Een bevraging kan bestaan uit het opvragen van informatie betreffende meerdere telefoonnummers en/of IP-adressen. Een volledig overzicht is opgenomen in bijlage 1: format toetsing steekproef.

Bevindingen:
Uit de steekproef komen een aantal bevindingen. We constateren dat in drie gevallen er geen dossier is aangetroffen. Eén post betreft een bevraging ten behoeve van een terreuroefening waarvoor een wettelijk kader ontbreekt.
De overige dossiers zijn getoetst op de aangegeven criteria. We constateren hierbij een aantal, met name administratieve, afwijkingen:
- In één geval is de vordering OvJ niet aangetroffen in Poli-OM. Bij navraag is aangegeven dat er sprake is van een fout in de registratie van het CIOT-ID.
- In vier gevallen ontbreekt het onderzoeksnummer of parketnummer op de aanvraag.
- In acht gevallen is geconstateerd dat er sprake is van een foutieve invoer van de rechtsgrondslag in CIS, in drie gevallen staat de naam of nummer van de aanvrager niet op het aanvraagformulier, maar is het formulier wel getekend door een opsporingsambtenaar.
- Bij twee spoedaanvragen buiten kantoortijd is de mail van de aanvrager niet in cc naar het GBK van de aanvragende eenheid gestuurd, maar is dit achteraf gedaan.
- In één geval is de bevoegde autoriteit en rechtsgrondslag niet opgenomen in de aanvraag. Dit betreft een aanvraag afkomstig vanuit de FIOD. Zie ook paragraaf 3.1.3.
- In twee gevallen is de rechtsgrondslag (artikel) niet ingevuld, maar alleen beschreven in de aanvraag.
- In twee gevallen ontbreekt de bronvermelding van de tap of historische verkeersgegevens.
- In achttien gevallen constateerden we een omissie in de aanvraag waarbij geen gebruik is gemaakt van de verplichte formats, een korte omschrijving van het wetsartikel ontbreekt, de bronvermelding van het telefoonnummer ontbreekt, de tap of historische verkeergegevens niet in de aanvraag is opgenomen of het doel van de bevraging niet is opgenomen in de aanvraag.

Bijlage 1: toetskader steekproef

CIOT-ID	
	Type aanvraag (OA, OvJ, SummIt, Spoed, 112, No Hit)
	Rechtsgrondslag
Grondslag	De vordering van een **opsporingsambtenaar** kan worden gedaan op basis van: - art 126 NA Sv (verdenking misdrijf) - art 126 UA Sv (georganiseerd verband) - art 126 ZI Sv (terroristisch misdrijf) - art 565 lid 2 Sv (vaststellen verblijfplaats van de aan te houden persoon) - art 11.10 lid 3 TW (alleen ivm melding "112")
	zijn onderstaande documenten aanwezig c.q. zijn de gevraagde gegevens ingevuld:
3.2. PV aanvraag CIOT bevraging opsp. Ambtenaar	aanvragen per mail met verplicht gebruik formats, ondertekend door de aanvrager en het procesverbaal is ingescand.
	Naam (pers.nr.) aanvrager aanwezig
	Identificerend kenmerk vermeld (Onderzoeksnummer)
	Handtekening opsporingsambtenaar aanwezig
	Rechtsgrondslag is ingevuld en komt overeen met toegestane wetsartikelen
	korte omschrijving overtreden artikel vermeld
	Bron van telefoonnummer (herkomst) aanwezig
	Personalia verdachte vermeld / indien onbekend NN
	Doel van de bevraging is vermeld
	Door aanvrager verlangde gegevens vermeld
	Komt de bevraging overeen met de aanvraag
	Er zijn geen handmatige aanpassingen gedaan op de aanvraag.
	Ruimte voor eventuele opmerkingen van de auditor:
Grondslag	**De vordering van een OvJ kan worden gedaan op basis van:** **- Art 126 N Sv (verkeersgegevens)** **- Art 126 U Sv (georganiseerd verband)** **- Art 126 II Sv (voorbereiding terroristisch misdrijf)** **- Art 126 ZH Sv (aanwijzingen terroristisch misdrijf)**
	zijn onderstaande documenten aanwezig c.q. zijn de gevraagde gegevens ingevuld:
3.3 Aanvraag CIOT Vordering OvJ	aanvraag per mail met verplicht gebruik formats of vanuit SummIt met txt bestand
	Naam of nr aanvrager aanwezig
	Identificerend kenmerk vermeld (Onderzoeksnummer)
	Parktenummer vermeld
	Bronvermelding van de tap of historische verkeersgegevens aanwezig
	Is vordering OvJ in PoliOm aanwezig
	Handtekening aanvrager aanwezig
	Rechtsgrondslag is ingevuld en komt overeen met toegestane wetsartikelen
	Komt de bevraging overeen met de aanvraag
	Er zijn geen handmatige aanpassingen gedaan op de aanvraag.
	Ruimte voor eventuele opmerkingen van de auditor:

CIOT-ID	
	Type aanvraag (OA, OvJ, SummIt, Spoed, 112, No Hit)
	Rechtsgrondslag
Grondslag	**Spoedbevragingen kunnen alleen worden gedaan als er sprake is van:** **a. Terreurdreiging** **b. Levensdelict** **c. Direct levensbedreigende situatie (in strafvorderlijke betekenis)** **d. Ontvoering / gijzeling** **e. Spoedtap**
	zijn onderstaande documenten aanwezig c.q. zijn de gevraagde gegevens ingevuld:
3.5.1. / 3.5.2. Spoed **Binnen kantoortijd**	mail met aanvraag (geen vast format)
	naam aanvrager vermeld.
	parketnr / BVH / BVH icm SummIt nr.
	Bevoegde autoriteit vermeld (Opsporingsambtenaar of OvJ)
	Rechtsgrondslag vermeld
	criterium spoed aangekruist
	Verlangde gegevens
	procesverbaal vordering verstrekking gebruikersgegevens binnen 72 uur opgesteld?
	Komt de bevraging overeen met de aanvraag
	Er zijn geen handmatige aanpassingen gedaan op de aanvraag.
	Ruimte voor eventuele opmerkingen van de auditor:
Grondslag	**Buiten kantooruren worden de spoedbevragingen uitgevoerd door I&S van de landelijke eenheid. Spoedbevragingen kunnen alleen worden gedaan als er sprake is van:** **- Terreurdreiging** **- Levensdelict** **- Direct levensbedreigende situatie (in strafvorderlijke betekenis)** **- Ontvoering / gijzeling** **- Spoedtap**
	zijn onderstaande documenten aanwezig c.q. zijn de gevraagde gegevens ingevuld:
3.5.1. / 3.5.2. Spoed	mail met aanvraag (geen vast format)
Buiten kantoortijd	naam aanvrager vermeld.
	de mail is in cc naar GBK aanvragende eenheid.
I&S	parketnr / BVH / BVH icm SummIt nr.
	Bevoegde autoriteit vermeld (Opsporingsambtenaar of OvJ)
	Rechtsgrondslag vermeld
	criterium spoed aangekruist
	Verlangde gegevens
	procesverbaal vordering verstrekking gebruikersgegevens binnen 72 uur opgesteld?
	Komt de bevraging overeen met de aanvraag
	Er zijn geen handmatige aanpassingen gedaan op de aanvraag.
	Ruimte voor eventuele opmerkingen van de auditor: