

To: [redacted] [redacted] [redacted] @rivm.nl; [redacted] [redacted] [redacted] @rivm.nl; [redacted] [redacted] [redacted] @rivm.nl; [redacted] [redacted] [redacted] @rivm.nl
Cc: [redacted] [redacted] [redacted] @rivm.nl
From: [redacted] [redacted]
Sent: Sat 1/16/2021 6:19:19 PM
Subject: RE: Doorst: Aankondiging weekendoverleg - IB&P bestelproces covid-vaccins
Received: Sat 1/16/2021 6:19:20 PM

Klopt [redacted] SNPG alleen voor bestellingen huisartsen, huisartsenposten en zorginstellingen.

From: [redacted] [redacted] <[redacted]@rivm.nl>
Sent: zaterdag 16 januari 2021 19:06
To: [redacted] [redacted] <[redacted]@rivm.nl>; [redacted] [redacted] <[redacted]@rivm.nl>; [redacted] [redacted] <[redacted]@rivm.nl>; [redacted] [redacted] <[redacted]@rivm.nl>; [redacted] [redacted] <[redacted]@rivm.nl>
Cc: [redacted] [redacted] <[redacted]@rivm.nl>
Subject: RE: Doorst: Aankondiging weekendoverleg - IB&P bestelproces covid-vaccins

Hoi [redacted]

Goed dat er voor het geheel een eerste ketenuitwerking is.
 Hierbij nog wat aanvullingen/opmerkingen:

Keten op hoofdlijnen:
 Volgens mij is SNPG webapp vooral voor huisartsen en zorginstellingen.
 Hosting SNPG webapp is bij direct- ICT. Partners 4IT doen het technisch- en applicatiebeheer.

Bij risico's zie kleur groen.

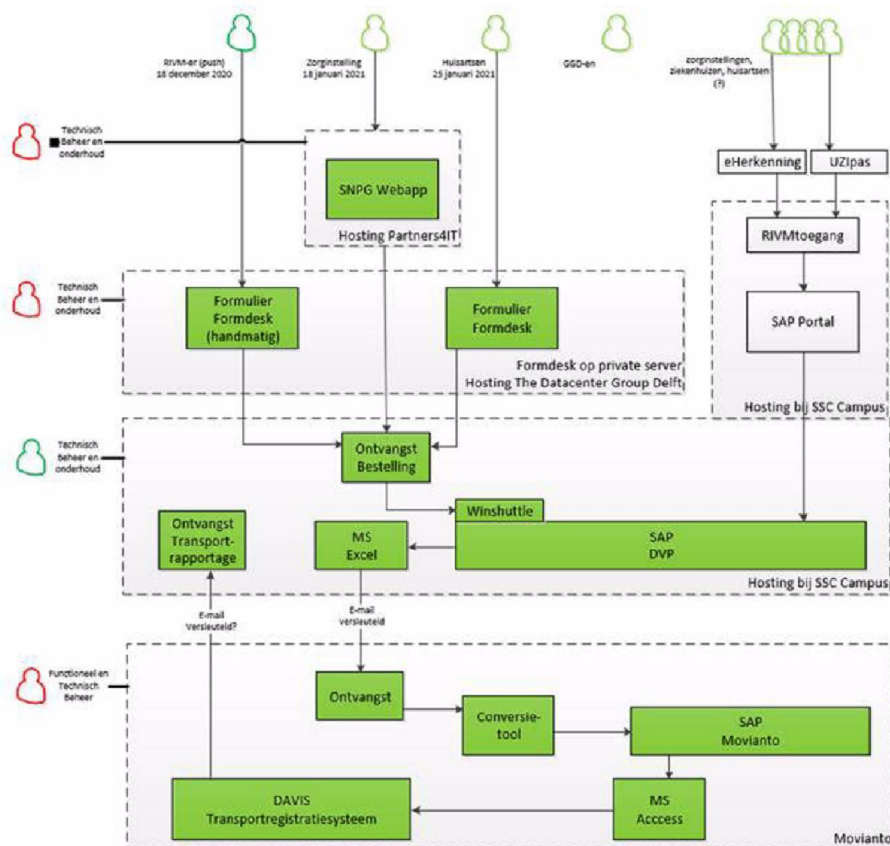
Met vriendelijke groet,
 [redacted]

RIVM [redacted] [redacted]
 [redacted] [redacted] (Volksgezondheid en Zorg)
 Tel.nr: [redacted]

From: [redacted] [redacted] <[redacted]@rivm.nl>
Sent: Saturday, January 16, 2021 09:46 AM
To: [redacted] [redacted] <[redacted]@rivm.nl>; [redacted] [redacted] <[redacted]@rivm.nl>; [redacted] [redacted] <[redacted]@rivm.nl>; [redacted] [redacted] <[redacted]@rivm.nl>; [redacted] [redacted] <[redacted]@rivm.nl>
Cc: [redacted] [redacted] <[redacted]@rivm.nl>
Subject: RE: Doorst: Aankondiging weekendoverleg - IB&P bestelproces covid-vaccins

Allen,

[redacted] heeft gisteren aangegeven morgen bereikbaar te zijn.
 Ondertussen heb ik het overzicht van de keten op hoofdlijnen gemaakt en een nieuw overzicht van de risico's voor nu(nog niet af). Zie hieronder.
 Graag jullie feedback.



Ref.	Omschrijving	Risico	Mitigerende maatregelen aanwezig	Te implementeren maatregelen
R-A	Dreiging statelijke actoren	<p>Dreigingen vanuit statelijke actoren manifesteren zich steeds meer. Dit o.a. gericht in de hoek van farmacie (hack bij Ema; documenten staan inmiddels op Russische fora) alsook op laboratoria (gerichte aanvallen op Belgische laboratoria).</p> <p>Indien informatie over bestellingen en/of transporten en/of</p>	<ul style="list-style-type: none"> • BBN3 dreigingsniveau toepassen op COVID-19 (gerelateerde) projecten, activiteiten en systemen. • Intensief contact met AIVD (NBV) en NCSC t.b.v. dreigingsinformatie en concrete aanwijzingen 	<ul style="list-style-type: none"> • Risicoanalyses uitvoeren op bestelketen op basis van BBN3 en maatregelen implementeren (of zo nodig accepteren) • Toepassen informatieclassificatie Departementaal Vertrouwelijk (DepV) en het bijbehorend normenkader hanteren; maatregelen implementeren (of zo nodig accepteren) <p>Voor nadere details zie beveiligingsniveau per systeem</p>

		<p>transportdetails misbruikt worden leidt dit direct tot imagoschade voor het RIVM. Ook is het mogelijk dat manipulatie van transporten of de vaccins zelf plaatsvindt. Ook mogelijk is het verspreiden van desinformatie op basis van onderschepte informatie welke is gemanipuleerd. Antivaxxers zijn ook mogelijke actoren.</p>	<ul style="list-style-type: none"> • Direct contact met ketenpartners opzetten/onderhouden • Verhoogde dijkbewaking in de vorm van o.a. monitoren op verdacht verkeer, verkeerde inlogpogingen etc. 	
R-B	Tijdsdruk en ad hoc besluitvorming	<p>Een aantal activiteiten binnen het programma zijn later dan gewenst van start gegaan. Daarbij is pas zeer recentelijk IB aangehaakt (eind december 2020). Vanaf 18 januari zal het bestelproces via de SNPG webapp gaan lopen voor de zorginstellingen (verpleeghuizen) met Pfizer en vanaf 25 januari de huisartsen met Moderna</p>	<ul style="list-style-type: none"> • Awareness creëren voor het dreigingsniveau en • Aanlevering van bestanden verloopt via verbinding die wel voorzien is van encryptie. • Bestanden worden na aanlevering op de SFTP server meteen doorgezet voor import en verwijderd (automatisch). • Toegang tot de SFTP server wordt gelogd. • Eerste periode is geen gebruik van CSV bestanden. • Bij de koppeling met BRBA worden deze wel voorzien van encryptie 	<ul style="list-style-type: none"> • Inzage in de keten en de afhankelijkheden
R-C	Beveiligingsniveau SNPG webapp	<p>De SNPG webapp gaat gebruikt worden Juist niet door door GGD-en en maar huisartsen en zorginstellingen,,, om COVID-19 vaccins te bestellen</p>	<ul style="list-style-type: none"> • Uitgevoerde risicoanalyse op SNPG webapp - BBN2 • Uitvoeren pentest en laten hertesten 	<ul style="list-style-type: none"> • Risicoanalyse uitvoeren op BBN3, maatregelen implementeren (of zo nodig accepteren) • Monitoren openstaande bevindingen pentest • ISO 27001 certificering

			<ul style="list-style-type: none"> • 	<p>partner 4IT</p> <ul style="list-style-type: none"> • SNPG is ISO 27001 gecertificeerd – toepasselijkheidsverklaring vragen?
R-D	Beveiligingsniveau Formdesk formulier COVID-19 bestellingen.	Ongeautoriseerde toegang	<ul style="list-style-type: none"> • Het aantal database administrators is beperkt. • Logging wordt aangeleverd bij SIEM/ • 	
R-E	Beveiligingsniveau SAP DVP en Winshuttle		<ul style="list-style-type: none"> • Voor de meeste systemen is automatische controle van de logfiles al actief. • Van de CIMS systemen worden de logbestanden aangeleverd bij SIEM/SOC van RIVM, maar wordt nog handmatig de rapportage beoordeeld (de eerste maand wekelijks na live gang). • Na in productie name van CIMS zal monitoring worden geautomatiseerd uiterlijk na een maand van live gang zodat afwijkingen nog sneller worden gedetecteerd. 	<ul style="list-style-type: none"> • Moeten we dit dan ook niet hebben voor het bestelproces of wordt dit ondervangen door de controle tbv CIMS
R-F	Beveiligingsniveau SAP Movianto	Movianto gaat nu de COVID-19 vaccins distribueren wat een groot aantal risico's met zich meebrengt. De bestelinformatie en de details over transporten	<ul style="list-style-type: none"> • Kennis maken, relatie opbouwen en een eerste inventarisatie uitvoeren van kwetsbaarheden 	<ul style="list-style-type: none"> * Check op DepV en uitvoeren risicoanalyse BBN3 • Interfacing (koppeling) tussen SAP RIVM en SAP Movianto realiseren • Logging en monitoring e.d. (SIEM-SOC functies) realiseren

		e.d. worden tussen RIVM en Movianto uitwisseld. In 2020 is vanuit NCTV is een assessment uitgevoerd i.r.t. de fysieke beveiliging. De risico's en maatregelen ten aanzien van informatie-beveiliging/cybersecurity zijn nog niet beoordeeld.	en verbeterpunten <ul style="list-style-type: none"> • Assessment door de AIVD (NBV) • 	i.s.m. NCSC of commerciële partij <ul style="list-style-type: none"> • ISO27001 certificering door Movianto • PM (o.a. uit rapport AIVD) •
R-G	Afgifte vaccins	In scope?	•	•

Met vriendelijke groet,

5.1.2e CISO team - CISM CISA CRISC RSE | CISSP
 5.1.2e
 m 5.1.2e out of office: 5.1.2e
 Complexity and confusion are the worst enemies of security

RIVM | Bureau Directieraad | CIO Office | www.rivm.nl
 De zorg voor morgen begint vandaag

Van: 5.1.2e <5.1.2e@rivm.nl>
Verzonden: zaterdag 16 januari 2021 08:43
Aan: 5.1.2e <5.1.2e@rivm.nl>; 5.1.2e <5.1.2e@rivm.nl>
CC: 5.1.2e <5.1.2e@rivm.nl>
Onderwerp: Doorst: Aankondiging weekendoverleg - IB&P bestelproces covid-vaccins
Urgentie: Hoog

Hallo 5.1.2e
 Zie onderstaand spoedverzoek.
 Ik denk dat jullie sleutel figuren zijn bij het voorbereidende gesprek.
 Is het mogelijk dat jullie aansluiten? Zondag 12:00?

Groet 5.1.2e

Van: 5.1.2e <5.1.2e@rivm.nl>
Datum: 15 januari 2021 om 18:47:39 CET
Aan: 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>
 <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>
CC: 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>, 5.1.2e <5.1.2e@rivm.nl>
Onderwerp: Aankondiging weekendoverleg - IB&P bestelproces covid-vaccins
Prioriteit: Hoog

Collega's,

Omdat na het overleg vanmorgen een aantal onduidelijkheden resteren m.b.t. de IB&P-bestelproces en omdat de DR graag wil begrijpen tegen welke restrisico's zij "ja" zegt, plan ik een weekendbijeenkomst in (zondag 17 januari 2021 van 12u tot uiterlijk 15u).

Proces zal onder leiding staan van 5.1.2e en ondergetekende. We werken toe naar een overzichtelijk

formulier waarmee e.e.a. uitgelegd kan worden. [5.1.2e] leveren om zondag 12u een nieuw overzicht aan van de stand van zaken van dat moment. Om 16u zondagmiddag vindt een nieuwe risicoacceptatie plaats, in aanwezigheid van de DG RIVM.

Ik stel voor dat [5.1.2e] en [5.1.2e] kortsluiten wie van hen namens DVP deelneemt en dat [5.1.2e] bepaalt wie namens CvB en met kennis van de SNPG-app deelneemt.

Het spijt me dat ik inbreuk maak op jullie weekend. Dit is op dit moment even niet anders. Dank voor jullie tomeloze inzet.

Met vriendelijke groet,

[5.1.2e]

[5.1.2e]

.....
Rijksinstituut voor Volksgezondheid en Milieu

Antonie van Leeuwenhoeklaan 9 | Postbus 1 | 3720 BA Bilthoven

.....
T

[5.1.2e]

M

[5.1.2e]

[5.1.2e]@rivm.nl

<http://www.rivm.nl>

.....
RIVM *De zorg voor morgen begint vandaag*