Council of the European Union

Brussels, 21 December 2022
(OR. en, nl)

16268/22

Interinstitutional File:
2022/0272(COD)

CYBER 416
JAI 1730
DATAPROTECT 378
TELECOM 541
MI 977
CSC 606
CSCI 209
IA 234
CODEC 2080
INST 471
PARLNAT 200

COVER NOTE

From:	The Senate of the Kingdom of the Netherlands
date of receipt:	13 December 2022
To:	General Secretariat of the Council
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 - [12429/22 - COM (2022) 454] - Opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find attached the above-mentioned document followed by a courtesy English translation.

Eerste Kamer der Staten-Generaal

Europese Commissie
De heer M. Šefčovič
Wetstraat 200
1049 Brussel
België

Kazernestraat 52
2514 CV Den Haag
postbus 20017
2500 EA Den Haag

telefoon 070 312 92 00
fax 070 312 93 90

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum *13 december 2022*
betreft *Voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten (COM(2022)454)*
ons kenmerk *172339U*

Geachte heer Šefčovič,

De leden van de vaste commissie voor Justitie en Veiligheid hebben in hun commissievergadering van 15 november 2022 beraadslaagd over het door de Europese Commissie voorgestelde Voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten[1]. De leden van de fracties van **GroenLinks**, **Partij van de Arbeid** (PvdA), de **Socialistische Partij** (SP) en de **Partij voor de Dieren** (PvdD) gezamenlijk hebben naar aanleiding van het voorstel enkele vragen. Ook het lid van de **Onafhankelijke Senaatsfractie** (OSF) heeft vragen naar aanleiding van het voorstel.

Vragen van de leden van de fracties van GroenLinks, PvdA en SP en PvdD gezamenlijk
De leden van de fracties van GroenLinks, PvdA en de SP gezamenlijk hebben met interesse kennisgenomen van het voorstel. Zij ondersteunen het uitgangspunt dat er duidelijke algemene kaders moeten komen voor de veiligheid van digitale producten en diensten. De leden hebben wel een aantal vragen over onder andere de impact van de verordening op vrije en opensourcesoftware en over de effectieve handhaving van het voorstel.

Vrije en open source software
De leden zijn blij om in considerans nummer 10 van het voorstel te lezen dat vrije en opensourcesoftware, die buiten het kader van handelsactiviteiten wordt ontwikkeld of geleverd, moet zijn uitgezonderd van toepassing van de verordening.[2] De leden constateren dat het ontwikkelen van vrije en open source software op een hele diverse manier gebeurt. Zij zijn daarom bang dat niet duidelijk genoeg afgebakend is wanneer er sprake is van vrije software, ontwikkeld of geleverd in het kader van een handelsactiviteit. Onderschrijft de Europese Commissie dat duidelijkheid voor opensource-ontwikkelaars omtrent toepasbaarheid van de verordening, essentieel is om te zorgen dat dit voorstel geen onvoorziene gevolgen heeft voor opensourcesoftware in Europa? Vanuit welke afwegingen is de Europese Commissie gekomen tot de tekst van het onderhavige voorstel?

[1] COM(2022)454.
[2] COM(2022)454, p. 16.

De leden zijn blij dat in de considerans nog een aantal voorbeelden is gegeven wanneer er sprake kan zijn van handelsactiviteit voor software. De leden horen graag of volgens de Europese Commissie de volgende voorbeelden in overwegende mate ook onder 'handelsactiviteit' zouden kunnen vallen:

1. Het ontvangen van vrijwillige, onvoorwaardelijke donaties door gebruikers van de software.
2. Het ontvangen van prestatieafhankelijke donaties ('feature bounties').
3. Ontwikkelaars die gesponsord worden, bijvoorbeeld door materialen te krijgen of reiskosten voor conferenties vergoed te krijgen.
4. Het gratis uitlenen van apparatuur ter bevordering van de ontwikkeling van de opensourcesoftware.

Daarnaast zullen er natuurlijk (grote) vrije en opensourcesoftwareprojecten zijn die wel onder de werking van de Cyber Resilience Act (CRA) zullen vallen. De leden vinden dat uiteraard niet bezwaarlijk; grote opensourceprojecten waar geld aan verdiend wordt, moeten immers ook veilig zijn. Wel zien zij in de uitvoering hiervan enkele onduidelijkheden. Wie is verantwoordelijk voor de naleving van de verplichtingen uit hoofdstuk 2 van het voorstel als een – door een collectief gemaakt – softwareproduct door een marktpartij 'op de markt' wordt gebracht[3], bijvoorbeeld door het verlenen van betaalde ondersteuningsdiensten?[4] Is dat dan de marktpartij die de ondersteuningsdiensten levert, het collectief van vrijwilligers die de software schrijft, of beide? Is het onder het huidige voorstel mogelijk dat een enkele vrijwilliger aansprakelijk gesteld wordt, omdat een andere partij software waaraan hij heeft bijgedragen in de handel brengt?

De leden vinden het belangrijk dat de zorgen van de vrije en opensourcesoftwaregemeenschap weggenomen kunnen worden en dat Unieburgers goed ingelicht wordt in welke gevallen een product of softwareproject onder de voorwaarden van dit voorstel zullen vallen. Dit om 'chilling effects' te voorkomen en de administratieve last te verlagen. Welke acties zal de Europese Commissie ondernemen om te zorgen dat de effecten van de verordening duidelijk zullen zijn en de administratieve lasten voor compliance overzichtelijk blijven voor de vrije en opensourcesoftwaregemeenschap? Zou de Europese Commissie een concrete handreiking kunnen doen aan de vrije en opensourcesoftwaregemeenschap door richtlijnen op te stellen wanneer, en in hoeverre, opensourcesoftwareprojecten binnen de reikwijdte van de verordening zullen vallen?

Onderstreept de Europese Commissie het belang van een gezonde en actieve opensourcesoftwaregemeenschap in Europa, zowel vanuit het perspectief om minder afhankelijk te zijn van software buiten Europa, als vanuit het perspectief van digitale innovatie? Zo ja, heeft de Europese Commissie acties ondernomen, of is zij van plan acties te ondernemen, om het speelveld voor opensourcesoftware en -hardware te verbeteren in de EU?

De leden merken ook op dat veel vrije en opensourcesoftware die gratis beschikbaar wordt gemaakt buiten handelsactiviteit vervolgens weer gebruikt wordt in commerciële producten door andere partijen. Veel software waar veel mensen (indirect) van afhankelijk zijn, worden (grotendeels) ontwikkeld door vrijwilligers. Heeft de Europese Commissie overwogen om in de CRA bepalingen op te nemen die fabrikanten die opensourcesoftware gebruiken aan te moedigen om vrijwillige upstream-opensourcesoftware-ontwikkelaars te ondersteunen in het realiseren van de verplichtingen uit de CRA? Zo ja, waarom is dit niet gerealiseerd? Zo nee, zou de Europese Commissie positief er tegenover staan om zulke prikkels toe te voegen aan de CRA?

---

[3] Artikel 3 (21), p. 37.

[4] Overweging 10, p. 16.

Handhaving
De leden vroegen zich af hoe zij de verhouding tussen de CRA en de voorgestelde vernieuwde productaansprakelijkheidsrichtlijn moeten zien. Op welke manier biedt de CRA dan wel de nieuwe productaansprakelijkheidsrichtlijn voldoende mogelijkheden voor eindgebruikers om nakoming van de verplichtingen uit de CRA af te dwingen?

Levensduur[5]
De leden zijn blij om te lezen dat de verordening een verplichting inhoudt om voor een bepaalde duur kwetsbaarheden op te lossen. De gekozen duur van ten hoogste vijf jaar, of de verwachte levensduur als dat korter is, vinden de leden echter onbegrijpelijk in het licht van de duurzaamheidsambities van de EU. Veel fysieke producten zijn immers volledig afhankelijk van veilige software. Een korte ondersteuningstermijn van de software op dergelijke producten kan onnodige verspilling in de hand werken. Waarom is er gekozen voor een zo algemene termijn, in plaats van een termijn die productafhankelijk is? En waarom is er specifiek gekozen voor een maximumtermijn van 5 jaar?

Daarnaast zullen gebruikers na het einde van deze wettelijke ondersteuningstermijn mogelijk gebruik willen blijven maken van het product met digitale elementen. Welke mogelijkheden biedt de CRA aan gebruikers om te zorgen dat ze ook na deze termijn veiligheidsupdates kunnen krijgen, eventueel van een andere partij dan de oorspronkelijke fabrikant? Hoe kijkt de Europese Commissie ernaar om een verplichting te stellen om broncode, inclusief voorbereidend materiaal zoals 'toolchains' en compilatiegegevens, na een bepaalde termijn beschikbaar te moeten stellen als een fabrikant geen veiligheidsupdates meer wil leveren?

Vragen van het lid van de fractie van de OSF
Het lid van de OSF heeft kennisgenomen van het voorstel om sectorbreed de digitale beveiliging te verhogen en daarmee de algehele ICT-infrastructuur minder kwetsbaar te maken. Hij ziet deze verordening als het toevoegen van het recht op cyberbeveiliging en stellen van een updateverplichting. Er zijn wel meerdere onduidelijkheden welke het lid graag meer verhelderd zou willen zien.

Spoorboekje
Aanvullend, welke route wordt geboden voor nationale initiatieven om ook op Europese schaal uitvoerbaar te worden? Hierbij kunnen we bijvoorbeeld denken aan (aanvullende) richtlijnen, implementaties en ook (subsidie)regelingen.

Voorziet de Europese Commissie de wens en de mogelijkheid om een bredere procedure te doorlopen? Hierbij kan gedacht worden aan bijvoorbeeld meervoudige consultatie of installatie van een adviesorgaan vanuit de sector. Een bredere procedure, mogelijk zelfs cyclisch, zou kunnen bijdragen aan de (door)ontwikkeling van de criteria en de sectorbrede voorlichting van de standaard die wordt nagestreefd. Ook om, in de reikwijdte van de CRA, in afstemming te blijven/brengen met andere Unie wetgevingsinstrumenten. Zo ja, hoe ziet de Europese Commissie dat dan voor zich?

Cyberbeveiliging betreft zeer specialistische kennis, terwijl volksvertegenwoordiging in veel gevallen een lekenbestuur is. Zeker op dit vakgebied. Op welke wijze wordt gewaarborgd dat de CRA als beleid ook uitvoerbaar zal zijn? Hoe wordt voorkomen dat deze verordening flopt? Er is veel geschaad vertrouwen als het gaat om overheden en haar ICT-projecten. Hoe wil de Europese Commissie haar geloofwaardigheid herwinnen/bewijzen, zodat ze ook sectorbreed steun krijgt om met deze verordening de cyberbeveiliging daadwerkelijk naar een hoger niveau te tillen?

Handhaving

[5] Artikel 23 (2), p. 51-52

In het voorstel blijft onduidelijk hoe en met welke reikwijdte en daadkracht de CRA zal worden gehandhaafd. In het arsenaal van middelen die nodig zouden kunnen zijn, zou ook kunnen geworden gedacht aan handelingen die (momenteel) voorbehouden zijn tot het nationale recht. Kan de Europese Commissie inzicht geven op de rechtsgevolgen die er kunnen voortkomen in de naleving van de CRA dan wel schenden van de CRA?

Startups en innovatie
De verordening verzoekt aanbieders om over te gaan tot certificering en het verkrijgen van een label. Zo ook voor startups en innovatie binnen de sectoren die onder deze verordening zullen vallen. Een zelfassessment van geschat 18.400 euro en/of een conformiteitsbeoordeling door een derde partij van geschat 25.000 euro kunnen worden gezien als aanzienlijke investeringen. Is de Europese Commissie voornemens om hierin een subsidieregeling te voorzien? Of zijn er uitzonderingsregels of verminderde reikwijdte te verwachten om de administratieve lasten te verfichten?

Daar waar Europese ontwikkelaars geconfronteerd worden met de CRA, is er een aannemelijke kans dat wereldwijd denkende spelers binnen de sector, innovatie buiten Europa gaan plaatsen. Is er bij de Europese Commissie inzicht in hoe de CRA invloed zal gaan hebben op arbeidsmarkt van de sector en onze globale positie binnen de kenniseconomie? En/of heeft de Europese Commissie vertrouwen in de realisatie van een wereldwijde standaard met deze verordening, waarmee ook niet-Europese aanbieders kunnen worden geconformeerd? Voorziet ze dat aanbieders de Europese markt (voorlopig) zullen gaan mijden, met gevolg van verminderd aanbod, keuzevrijheid en maatwerk?

Eerlijke concurrentie
De nalevingskosten worden als 2% van de omzet geschat. Berekening: 29 miljard ten opzichte van 1485 miljard. Omdat een zelfassessment of conformiteitsbeoordeling geschat wordt op 18,4 tot 25 duizend euro, kan daarmee worden afgeleid dat voor dit specifieke certificaat er een omzet van boven de 1 miljoen euro als marktcomfort wordt ingeschaald. Heeft de Europese Commissie toezichthouders op de markten om een zienswijze gevraagd?

Financiële consequenties
Qua financiële consequenties voor de nationale overheid en/of medeoverheden, evenals de gevolgen van regeldruk voor bedrijfsleven en de burger worden miljardenbedragen voorzien. Zowel voor kosten als voor kostenbesparing. Zodra de gevolgen van de invoering van deze verordening duidelijk worden, is de Europese Commissie voornemens om hiervoor een compensatieregeling in te richten? Zo ja, welke doelgroepen (zoals gemeenten of midden- en kleinbedrijf) en om welke redenen, zullen dan worden gecompenseerd? Op welke wijze zal dit in de begroting worden ingepast en/of hoe zal dit herleidbaar zijn?

Gijzeling van gegevens en systemen
In de laatste jaren worden ook overheden en publieke instellingen geconfronteerd met cyberbeveiligingsincidenten. Kan de Europese Commissie aangeven hoe deze situaties (door de verordening) voorkomen hadden kunnen worden? Welke criteria worden gehanteerd, ook bij werkwijzen wanneer gegevens gegijzeld worden en systemen overgenomen?

Actieve uitbating zwakheden door derden
Met de oorlog in Oekraïne is Europa wakker geschud dat er ook een digitaal front is. Hoe wil Europa deze verordening inzetten om zich te wapenen in de 'digitale oorlog'? Welke beperkingen en/of vrijheden van de nationale veiligheids- en inlichtingendiensten komen met de CRA in een ander daglicht te staan?

Bescherming van klokkenluiders en ethische hackers
Zwakten in systemen worden altijd door mensen ontdekt. Leveranciers hebben economische belangen bij het (ogenschijnlijk) ontbreken van zwakheden. Op welke wijze worden klokkenluiders en ethische hackers mede door deze verordening in bescherming genomen?

De leden van de vaste commissie voor Justitie en Veiligheid zien uw reactie met belangstelling tegemoet.

Hoogachtend,

mr. drs. M.M. de Boer
Voorzitter van de vaste commissie voor Justitie en Veiligheid

European Commission
attn. Mr M. Šefčovič, Vice-President for Interinstitutional Relations
and Foresight
Wetstraat 200
1049 Brussels
Belgium

date *13 December 2022*
subject *Proposal for a Regulation on horizontal cybersecurity requirements (COM(2022) 454)*
our reference *172339U*

COURTESY TRANSLATION

Dear Mr Šefčovič,

In their committee meeting of 15 November 2022, the members of the standing committee for Justice and Security of the Senate of the States General discussed the European Commission's proposal for a Regulation on horizontal cybersecurity requirements (also known as the Cyber Resilience Act).[1] The members of the parliamentary parties of the GreenLeft Alliance (**GroenLinks**), the Labour Party (**Partij van de Arbeid/PvdA**), the Socialist Party (**Socialistiche Partij/SP**) and the Animal Rights Party (**Partij voor de Dieren/PvdD**) together have a number of questions about the proposal. The member of the parliamentary party of the Independent Senate Group (**Onafhankelijke Senaatsfractie/OSF**) also has questions about the proposal.

Questions jointly raised by the members of the GroenLinks, PvdA, SP and PvdD parliamentary parties

The members of the GroenLinks, PvdA, SP and PvdD parliamentary parties have taken note with interest of the proposal. They support the principle that there should be clear general frameworks for the security of digital products and services. However, the members have a number of questions, for example about the impact of the Regulation on free and open-source software and about the effective enforcement of the proposal.

Free and open-source software

The members are pleased to note that recital 10 of the proposal states that free and open-source software, developed or supplied outside the course of a commercial activity should not be covered

[1] COM(2022) 454.

by the Regulation.[2] However, they would point out that the development of free and open-source software is carried out in very diverse ways. They are therefore concerned that what constitutes free and open-source software developed or supplied in the course of a commercial activity is not sufficiently clearly defined. Does the European Commission agree that it is essential for open-source software developers to be given clarity about the applicability of the Regulation in order to ensure that it has no unforeseen consequences for open-source software in Europe? What were the considerations that led the Commission to adopt this text of the present proposal?

The members are pleased that the recitals also give a number of examples of what may constitute a commercial activity in the case of software. They would like to know whether the European Commission considers that the following examples could also be largely covered by the term 'commercial activity':

1. receipt of voluntary and unconditional donations from users of the software;
2. receipt of performance-related donations ('feature bounties');
3. sponsorship of developers, for example in the form of materials received or the reimbursement of travel expenses when attending conferences;
4. the free loan of equipment to promote the development of open-source software.

Naturally, there will also be (large-scale) free and open-source software projects that do fall within the scope of the Cyber Resilience Act (CRA). The members do not, of course, find this objectionable: after all, large-scale open-source projects that are money spinners must also be secure. However, the members consider that some aspects of how this is to be implemented are unclear. Who is responsible for compliance with the obligations in Chapter II of the proposal if a software product made by a collective is 'placed on the market' by a market participant[3], for example by a firm that provides paid support services?[4] Is it the market participant which provides the support services, is it the collective of volunteers who write the software, or is it both? Is it possible under the current proposal for a single volunteer to be held liable because the software to which he contributed is being marketed by a third party?

The members consider it important for the concerns of the free and open-source software community to be addressed and for Union citizens to be properly informed about when a product or software project will fall under the terms of this proposal. This is to prevent chilling effects and alleviate the administrative burden. What action will the European Commission take to ensure that the effects of the Regulation are clear and that it remains possible for the free and open-source software community to gauge the administrative burden of complying with its provisions? Could the Commission provide concrete assistance to the free and open-source software community by drawing up

[2] COM(2022) 454, p. 15.
[3] Article 3 (21), p. 34.
[4] Recital 10, p. 15.

guidelines on when, and to what extent, open-source software projects will fall within the scope of the Regulation?
Does the European Commission endorse the importance of a healthy and active open-source software community in Europe, both from the perspective of reducing dependence on software from outside Europe and from the perspective of digital innovation? If so, has the Commission taken, or is it planning to take, any measures to create a more level playing field for open-source software and hardware in the EU?

The members would also point out that much open-source software that is made available free of charge on a non-commercial basis is subsequently used in commercial products by third parties. Much software on which many people depend (directly or indirectly) is to a large extent developed by volunteers. Has the European Commission considered including provisions in the CRA encouraging manufacturers that use open-source software to support voluntary upstream open-source software developers in complying with the obligations of the CRA? If so, why has it not implemented them? If not, would the Commission be in favour of adding such incentives to the CRA?

Enforcement
The members wonder how they should view the relationship between the CRA and the proposal for a revised Product Liability Directive. In what way does the CRA or the new Product Liability Directive provide sufficient options for end users to enforce compliance with the obligations under the CRA?

Product lifetime[5]
Members are pleased to note that the Regulation includes an obligation to remediate vulnerabilities for a specified period of time. However, given the EU's sustainability ambitions, they are puzzled by the chosen term of a maximum of five years or the expected product lifetime, if shorter. After all, many physical products are completely dependent on secure software. If the software on such products is supported for only a short period, this can lead to unnecessary waste. Why was a general term chosen rather than a product-dependent term? And what was the specific reason for choosing a maximum period of 5 years?

Moreover, users may wish to continue using a product with digital elements after the end of this statutory support period. What options does the CRA offer users to ensure that they can continue receiving security updates after the end of this period, possibly from a source other than the original manufacturer? How would the European Commission view the idea of making it obligatory for a manufacturer to make source code, including preparatory material such as toolchains and compilation data, available after a certain period of time if it no longer wishes to provide security updates?

[5] Article 23 (2), p. 47.

Questions raised by the member of the OSF parliamentary party

The member of the OSF parliamentary party has taken note of the proposal to increase digital security across the entire sector and thus make the overall ICT infrastructure less vulnerable. He sees this Regulation as conferring the right to cybersecurity and imposing an update obligation. However, he would like to have more clarification about a number of aspects that are unclear.

Scenarios

By way of addition, what route is offered to ensure that national initiatives are feasible on a European scale as well? Examples would be (additional) directives, implementing legislation and also (subsidy) schemes.

Does the European Commission consider that having in place a broader procedure would be desirable and feasible? This could include, for example, multiple consultations or the establishment of an advisory body drawn from the sector. A broader procedure, possibly even cyclical, could help in developing or continuing to develop the criteria and the provision of sector-wide information about the standard that is being pursued. And also help, within the scope of the CRA, to ensure that the procedure is and remains aligned with other EU legislative instruments. If so, how does the Commission envisage this happening?

Cybersecurity requires highly specialised knowledge which members of parliament tend to lack. This lack of expertise is especially true of this field. What has been done to ensure that the CRA will also be capable of being implemented as a policy? And what has been done to prevent this Regulation from flopping? Much trust has been lost when it comes to governments and their ICT projects. How does the European Commission intend to restore or prove its credibility, so that it also obtains sector-wide support enabling it to elevate cybersecurity to a higher level with this Regulation?

Enforcement

How the CRA is to be enforced and what will be the scope and strength of the enforcement action remains unclear in the proposal. The arsenal of resources that could be necessary could include measures that are currently the preserve of national law. Can the European Commission shed light on the legal consequences that may arise from compliance or non-compliance with the CRA?

Start-ups and innovation

The Regulation invites providers to proceed with certification and obtain a label. This also applies to start-ups and innovation within the sectors that will fall under this Regulation. A self-assessment costing an estimated EUR 18,400 and/or a third party conformity assessment costing an estimated EUR 25,000 can be regarded as sizeable investments. Does the European Commission intend to provide a subsidy scheme for this purpose? Or does it envisage introducing rules on exceptions or narrowing the scope of the Regulation to ease the administrative burden?

While European developers will be faced with the CRA, there is a good chance that globally oriented players within the sector will locate their innovation activities outside Europe. Does the European Commission have any idea of how the CRA will affect the sector's labour market and our global position within the knowledge economy? And/or is the Commission confident that this Regulation will result in the adoption of a worldwide standard with which non-European providers too may be obliged to comply? Does the Commission envisage a situation in which providers avoid the European market for the time being, owing to constraints on supply, freedom of choice and the provision of a customised product?

Fair competition

Compliance costs are estimated to be 2% of turnover. This gives a figure of EUR 29 billion on a total turnover of EUR 1,485 billion. As the cost of a self-assessment or conformity assessment is estimated to be between EUR 18.4 thousand and EUR 25 thousand, it can be deduced that for this certificate a turnover in excess of EUR 1 million is regarded as in line with market rates. Has the European Commission asked market surveillance authorities for their views?

Financial consequences

The financial consequences for central government and/or other government bodies as well as the consequences of regulatory pressure for the business community and the general public are expected to run into the billions. This is true of both costs and cost savings. Once the consequences of introducing this Regulation become clear, does the European Commission intend to set up a compensation scheme for this? If so, what target groups (such as municipal authorities or SMEs) will be compensated and for what reasons? How will this be incorporated into the budget and/or how will it be traceable?

Ransomware attacks on data and systems

In recent years, government bodies and public institutions too have had to deal with cybersecurity incidents. Can the European Commission indicate how such situations could have been prevented (for example by the Regulation)? What criteria are used, for example in procedures employed to counter ransomware attacks designed to access data and assume control of systems?

Active exploitation of weaknesses by third parties

The war in Ukraine has awakened Europe to the fact that there is also a digital front. How does Europe propose to use the Regulation to arm itself in the 'digital war'? On what restrictions on and/or freedoms of the national security and intelligence services does the CRA shed a different light?

Protection of whistle-blowers and ethical hackers
Weaknesses in systems are always discovered. Suppliers have an economic interest in ensuring that systems appear to have no weaknesses. How does this Regulation help to protect whistle-blowers and ethical hackers?

The members of the standing committee for Justice and Security await your reply with interest.

Yours sincerely,

M.M. de Boer
Chair of the standing committee for Justice and Security