Q&A Coordinated Vulnerability Disclosure

1. **Is the Manifesto legally binding?**
   The Manifesto is not a legally binding document. It is a declaration of intention. By signing the Manifesto companies signal that they support the principle of coordinated vulnerability disclosure and are committed to implementing the best practices described in the Manifesto.

2. **Why Should my company sign the Manifesto?**
   Companies who support the principle of coordinated vulnerability disclosure can show their support by signing and thereby contribute to a safer cyber world.

3. **Wat must my company do when it has signed the Manifesto?**
   After signing, companies should take measures to implement the best practices as described. Such as creating the possibility of notification and rewarding the person who notifies.
   Companies can also publically embrace the principles of the Manifesto by posting a news item on their website that they have signed.
   For further reference and an example of how organizations can implement the best practices: http://www.cio-platform.nl/uploads/CioPublicatie2016%20CegInfoSec%20Coordinated%20Vulnerability%20Disclosure%20Implementation%20Guide%20-%20ENG%20v1.0.pdf
   This is one example of implementation, organizations can choose any form of implementation that is suitable for their situation.

4. **What will happen next?**
   The Global Forum on Cyber Expertise has embraced this initiative and will be keeper of a record of organizations that have signed the Manifesto. In coming years, the objective for the Manifesto is to reach a still wider audience and gain more support for Coordinated Vulnerability Disclosure. Organizations that have signed the Manifesto will be recognized for their commitment.

5. **Will signing the Manifesto cost my company any money?**
   The signing of the Manifesto itself does not lead to any costs. Implementing the best practices may require (financial) resources. However, coordinated vulnerability disclosure will bring benefits to the organization, both material and immaterial such as less security incidents and reputation damage.

6. **Will those organizations that sign the Manifesto be registered in a public record?**
   Yes. The Global Forum on Cyber Expertise will be the keeper of a public register.

7. **Can my company still sign the Manifesto after May 12 2016?**
   Yes, organizations can sign the Manifesto at any time they wish. The GFCE will record this.

8. **Can my company sign the Manifesto and be recognized as such without attending the event in Amsterdam in person?**
   Yes. If your organization is unable to send a representative to Amsterdam to attend the event, signing is still possible and much appreciated. If your organization signs the Manifesto in advance of May 12, it will be mentioned at the event. If you want to sign in absence, please use this document and send it to vulnerability.disclosure@ncsc.nl

9. **The Manifesto refers to Terms and Conditions. What does this mean?**
   From the Manifesto: "*Taking in account that the finder of the vulnerability:*
   ** will agree on terms and conditions for disclosure of vulnerabilities found."*

   Companies that commit to coordinated vulnerability disclosure are free to decide on terms and conditions that suit their organization. Organizations may have different needs and therefore should design their own rules surrounding coordinated vulnerability disclosure. For further reference and an example of terms and conditions please visit: http://www.cio-platform.nl/uploads/CioPublicatie2016%20CegInfoSec%20Coordinated%20Vulnerability%20Disclosure%20Implementation%20Guide%20-%20ENG%20v1.0.pdf

10. **The Manifesto refers to combining efforts to follow international standards. What does this mean?**
    From the Manifesto: *"Combine efforts to follow international standards and best practices for remediating and disclosing vulnerabilities and implementing these in their organization. A non-comprehensive list with information on such standards and best practices can be found in Appendix A."*

    Companies that commit to coordinated vulnerability disclosure acknowledge the value of following international standards and best practices and of sharing and learning from each other when implementing these standards. Organizations may have different needs and therefore are free to decide if and with whom, how, and when to coordinate with other companies.