6 RECOMMENDATIONS

This investigation shows that vulnerabilities in software lead to insecurities for organizations that use software, and for those who depend on these organizations. The gap between digital dependency and the threat level on the one hand; and the extent to which society is resilient to it on the other hand, is growing. Fast and fundamental interventions are needed to prevent society from being disrupted. That is why the Dutch Safety Board issues recommendations. The first recommendation aims to increase response capacity in the short term. The recommendations that follow aim, in the longer term, to strengthen the public and private system and introduce incentives to create a system in which manufacturers and buyers of software work continuously to make software safer and more secure.

To the Dutch Cabinet and to organizations in the Netherlands that use software:[226]

1. Ensure in the near future that all potential victims of cyber attacks are alerted quickly and effectively – solicited and unsolicited - so they can take measures for their digital safety and security. To this end, bring together public and private response capacity and ensure sufficient mandate and legal safeguards.

Note: In any case, this concerns information about which systems of which organizations are vulnerable and at risk of being attacked (so-called 'victim information'). Currently, the legal interpretation of the GDPR (IP addresses as personal data) and the Dutch Security of Network and Information Systems Act (Wbni) (mandate of the NCSC limited to national government and vital operators) prevents the National Cyber Security Centre (NCSC) from warning all victims they receive information about, and from proactively collecting this information (scanning).

To the European Commissioner for Internal Market and the European Commissioner for A Europe Fit for the Digital Age:

2. Ensure that your initiatives to legislate for safer and more secure software lead to a European regulation that establishes the responsibility of manufacturers and provides insight to buyers of software in how manufacturers assume this responsibility. Establish that manufacturers are liable for the consequences of software vulnerabilities.

Note: Essential elements of this regulation include – but are not limited to – mandatory participation in bug bounty programmes, guidelines for independent audits, vulnerability reporting, traceability, recalls, and the sharing of lessons learnt from cyber attacks.

226 For practical reasons, the Dutch Safety Board addresses the government in its role as user of software through the State Secretary of the Interior, the Interprovincial Consultative Council, the *Vereniging van Nederlandse Gemeenten* (Association of Netherlands Municipalities), and the *Unie van Waterschappen* (Union of Water Boards). The other organizations, including health care, education, vital operators and other businesses, are addressed by the Dutch Safety Board through employers' organizations involved in the SER, such as: VNO-NCW, MKB-Nederland and LTO Nederland.

Legislation such as the GDPR has proven that European regulations in the digital domain are feasible and effective.

To software manufacturers collectively:[227]

3. Develop good practices with other manufacturers to make software safer and more secure. Include a commitment to these practices in contracts with your customers.
4. Warn and help all your customers as quickly and effectively as possible when vulnerabilities in software are identified. Create the preconditions necessary to be able to warn your customers.

Note: The responsibility and possibilities for making software safer and more secure, and for warning customers primary lies with the manufacturers themselves.

To the State Secretary of the Interior and Kingdom Relations and the Minister of Economic Affairs and Climate Policy (for the benefit of all organizations and consumers in the Netherlands)[228]*:*

5. Encourage that Dutch organizations and consumers jointly formulate and enforce safety and security requirements for software manufacturers. Ensure that the government plays a leading role in this. Proceed on the basis of the principle: collective cooperation where possible, sector-specific where necessary.

Note: It is necessary for buyers of software to join forces in order to strengthen their position towards manufacturers and jointly deploy the scarce cybersecurity expertise as efficiently and effectively as possible. A number of Dutch banks is already cooperating in this matter.

To the Dutch Cabinet:

6. Create a legal basis for the management of digital safety and security by the government, by analogy of the Dutch Government Accounts Act (Comptabiliteitswet).
7. Require all organizations to uniformly account for the way in which they manage digital safety and security risks.[229]

Note: The way in which governments and companies manage and account for the risks that are associated with digitization is as yet noncommittal. Fragmentation of responsibilities impairs decisive action. It is essential that a comprehensive system is put in place to help organizations to manage digital safety and security in a systematic and effective manner. Possible elements include an unambiguous mandate for government CISOs, supervision that is entrusted to the minister responsible, and mandatory accountability for all organizations regarding the management of digital safety and security risks, through annual reports and as part of the auditor's report.

227 This recommendation is addressed to all software manufacturers. For practical reasons, the Dutch Safety Board addresses the manufacturers involved in the incidents described in this investigation, the communities of the open source projects involved and the (members of the) Business Software Alliance trade association.

228 See footnote 2. Because of the relevance of safe and secure software to end users (including consumers), the *Consumentenbond* (Consumers' Association) will also be addressed. And the Chamber of Commerce for support to organizations

229 It is within reason to align with existing structures and obligations in the 2016 *Comptabiliteitswet* (applicable to governments), Civil Code (non-listed legal entities), further regulations on auditing and other standards (NV COS) from the NBA and harmonized legislation for public limited companies from the European Union.