THE DUTCH
SAFETY BOARD

SUMMARY

THE DIGINOTAR INCIDENT

Why digital safety fails to attract enough attention from public administrators

THE DIGINOTAR INCIDENT
Why digital safety fails to attract enough attention from public administrators

The Hague, 28 June 2012

The Dutch Safety Board's reports are in the public domain.
All reports are also available on the Safety Board's website www.safetyboard.nl

THE DUTCH SAFETY BOARD

The aim in the Netherlands is to reduce the risk of accidents and incidents as much as possible. If accidents or near-accidents nevertheless occur, a thorough investigation into the causes of the problem, irrespective of who is to blame for it, may help to prevent similar problems from occurring in the future. It is important to ensure that the investigation is carried out independently from the parties involved. This is why the Dutch Safety Board itself selects the issues it wishes to investigate, mindful of citizens' position of dependence with respect to public authorities and businesses. In some cases, the Dutch Safety Board is required by law to conduct an investigation.

	Dutch Safety Board		
Chairman:	T.H.J. Joustra Annie H. Brouwer-Korf F.J.H. Mertens E.R. Muller J.P. Visser		
General secretary:	M. Visser		
Visiting address:	Anna van Saksenlaan 50 2593 HT The Hague, The Netherlands	Correspondence address:	PO Box 95404 2509 CK The Hague
Telephone:	+31 (0)70 333 7000	Fax:	+31 (0)70 333 7077
Internet:	www.safetyboard.nl		

This report is published in Dutch and English. In the event of any discrepancy between these versions, the Dutch text shall prevail.

CONSIDERATION

The rapid rate at which Dutch society is digitising means that digital safety is becoming increasingly important. The government has a special responsibility to secure the digital data for which it is responsible. Whereas, among themselves, private individuals and companies are free to choose the parties with which they exchange or do not exchange their data, the government obliges private individuals and companies to make data available. Private individuals and companies must therefore be able to rely on the government undertaking every possible effort to prevent the loss and misuse of that data.

Digital certificates constitute an important instrument in providing this protection. The DigiNotar hack and its aftermath raised questions about the extent to which the trustworthiness of digital certificates is safeguarded. Moreover, shortly after the incident, there was a commotion about the general state of safety of, among other things, the websites and networks of municipal authorities. Both events prompted the Dutch Safety Board's concern as to the extent to which and the way in which public authorities actually fulfil their responsibility for the digital safety of private individuals and companies.

As evidenced by the number of investigations into digital safety and the reliability of services concerning digital certificates that it has ordered, the government shares this concern. The Dutch Safety Board was asked by the Minister of the Interior and Kingdom Relations and the Minister of Security and Justice to carry out an investigation. In view of the importance of digital safety and the special responsibility of the government to safeguard that safety, the Dutch Safety Board agreed to the request. The Dutch Safety Board is of the opinion that lessons should be learned from the DigiNotar incident so that public authorities can improve their actions to safeguard digital safety.

The Dutch Safety Board's investigation explored how public authorities safeguard digital safety at administrative level and identified problem areas in this context. In addition, it considered the role of the government as a creator of enabling conditions for digital safety. In this context, the Dutch Safety Board focused primarily on the reliability of digital certificates and the role played by the government in this regard.

The hacking of DigiNotar and its consequences
In June and July of 2011, a hacker accessed the computer systems of DigiNotar B.V. This company provided digital certificates to protect electronic data traffic with, as well as relating services. The hacker succeeded in generating and issuing fraudulent certificates. As a result, the data of private individuals and companies was at risk of being intercepted, which can lead to misuse of data, privacy breaches, identity fraud and financial loss.

The supply, making available and use of digital certificates takes place within a system that consists of agreements, parties and technologies and is referred to as a 'public key infrastructure' (PKI). The structure of a PKI is aimed at ensuring that a certificate service provider (CSP) that is no longer trusted is removed from the system. In the event of removal, the certificates issued by the CSP concerned, become unusable and parties must switch to the certificates of a different CSP. In the case of the DigiNotar hacking incident, it unexpectedly turned out that this safety measure could not be taken without serious complications. Rendering all certificates issued by DigiNotar unusable would place the continuity of various essential data flows with and between public authorities at great risk. Such a loss of continuity could have led to substantial economic damage and social disruption.

Among other things, DigiNotar supplied so-called PKIoverheid certificates. These certificates are intended for the protection of electronic data traffic with and between public authorities. The Dutch state is guarantor with respect to the reliability of these certificates. Following the hacking incident, however, the Dutch state could no longer guarantee that private individuals or companies could safely communicate with public services by means of the PKIoverheid certificates supplied by DigiNotar.

The DigiNotar incident could take place because the government organisations involved assumed that the company's certificate services were sound. The commissioning authority on behalf of the Minister of the Interior and Kingdom Relations, Logius, and the supervisor, the Independent Post and Telecommunications Authority (OPTA), relied primarily on the company and auditing by an external auditor. These government organisations were therefore aware of DigiNotar's actual business operations only to a limited extent, even though it was a company that provided safety critical services of relevance to vital government interests.

Public authorities also do not appear to have actually taken into account the possibility of a certificate service provider like DigiNotar being compromised, as a result of which no proper, proportional measures were in place to effectively control the consequences of such an event. Ultimately, massive social disruption that the events at DigiNotar could have caused was successfully prevented, largely due to the ability to improvise of the government organisations involved.

Measures already taken and other investigations
The events at DigiNotar were a wake-up call to many within the government and led to a broad range of initiatives aimed at improving the ability to cope with similar events in the future. Since the incident, digital safety has been a clear area of focus of the government, parliament and many other public authorities.

The government ordered several investigations into certificate services. These investigations led to the announcing of various measures aimed at improving the safety of data traffic with and between government organisations, such as a tightening of the PKIoverheid Terms of Reference, a clearer allocation of roles among the parties involved and stricter supervision by OPTA and Logius. The Dutch Safety Board believes that these measures make good sense. At the same time, however, the Dutch Safety Board is of the opinion that a lasting improvement of digital safety can only become a reality if the underlying problems are also addressed. More is required to achieve this aim than the measures already announced by the government.

The Dutch Safety Board investigated why the parties involved acted so trustingly with regard to the functioning of the digital certificates system. In a situation in which the public interest is at stake, such trust is remarkable and risky. The answer to this question is the key to improving the Dutch government's digital safety. The Dutch Safety Board distinguishes two important factors.

Insufficient risk awareness among administrators
First, the Dutch Safety Board finds that the parties involved in PKIoverheid were insufficiently aware of factors that could put the reliability of digital certificates at risk. Prior to the hacking of DigiNotar, neither the Minister of the Interior and Kingdom Relations as the party responsible for the system, nor the other parties involved, had considered how the reliability of digital certificates, and therefore the safety of electronic data traffic, might be compromised. Because the risks were not actually known, not enough preventive measures had been taken. Moreover, the measures that were in place to deal with incidents proved to be inadequate and extremely risky. Implementation of the scenario provided for could have led to a large-scale failure of essential data flows and, as a result, to social disruption.

In supplement to the investigation of the DigiNotar hack, an exploratory investigation of a number of public authorities has been carried out. It revealed that municipalities in general lack sufficient awareness of the risks that threaten digital safety. Risks are systematically identified, listed and controlled by means of safety management procedures only with respect to the municipal personal records database, to which stringent legal requirements apply. The systematic safeguarding of digital safety takes place to a far lesser extent in other data processing operations, however. Risk awareness is mainly present at the level of the ICT department. It is virtually non-existent at the top level of the administrative organisation or in the Municipal Executive.

In some public services, such as the Tax and Customs Administration and the Social Insurance Bank, a more active risk management with respect to safeguarding digital safety has been found. Undisturbed digital data processing is crucial to the operations of these organisations. ICT and safety is therefore an area to which they give considerable operational and administrative attention.

Executive inability to take responsibility
Second, the investigation revealed that there are major differences in the way in which public authorities safeguard digital safety in administrative and organisational terms. The Dutch Safety Board found stronger administrative and organisational involvement in digital safety at organisations where data processing is a central part of the primary process, such as at the Social Insurance Bank and the Tax and Customs Administration, than at organisations where data processing is less central. At these latter organisations, public executives are generally not involved in safeguarding digital safety, whereas the Dutch Safety Board believes that such involvement is necessary. The only become involved personally in the event of major incidents like the hacking of DigiNotar or the 'Lektober Action', when the 'Webwereld' website of IDG Nederland published a daily privacy leak under the name 'Lektober' ('leaktober') during the entire month of October 2011 to draw attention to the safety of privacy-sensitive data.

Recent incidents make public executives increasingly aware that digital safety is a matter that cannot be left exclusively to an ICT department to deal with. Achieving digital safety requires more than just technical solutions. First and foremost, decisions as to the way in which and the level up to which risks to digital safety are to be identified and controlled must be made at the administrative level. Public executives do not always feel capable of fulfilling their responsibility for digital safety, however. They often lack the knowledge required to effectively manage the systematic control of risks to digital safety or even to determine what information they require from the organisation for this purpose. It is important for public executives to have sufficient understanding of the relevant aspects of digital safety. This way, they can ask the right questions and make sure that digital safety is adequately safeguarded in their organisation.

The lack of understanding of digital safety described above results in poor governance of digital safety. Public executives should be able to formulate objectives and set requirements and verify whether those are met, if they are to assume true responsibility for activities carried out under their authority. This is true both within and across organisations. Many are currently unable to do so. As a result, digital safety is often left to those who are responsible for it at the operational level. The Dutch Safety Board is of the opinion that public executives should assume their responsibility to safeguard digital safety more explicitly. Some of the recommendations set out in this report are aimed at ensuring that this will indeed be done.

What is needed
The DigiNotar incident led to a broad range of initiatives aimed at improving the ability to cope with a similar situation in the future. In view of the above, the Dutch Safety Board believes that the main priority is for public executives to assume responsibility and exercise control more explicitly with respect to digital safety. The recommendations set out in this report are therefore aimed at making digital safety a key concern, requiring a degree of administrative involvement similar to, for example, financial management.

To achieve the change described above, public executives have to truly assume final responsibility and be held accountable for digital safety. In order for control to be exercised, there must be a sufficient degree of insight into and knowledge about digital safety at the executive level.

The only way of ensuring the best possible control of risks is by applying information safety management. In the Dutch Safety Board's opinion, this means that the risks associated with digitisation are identified, listed and evaluated, that measures are taken to reduce the risks to the greatest extent possible. These steps must constitute a permanent part of the organisational process. Holding public executives accountable for digital safety may encourage them to develop and apply the kind of policy required in this regard.

Special attention should be given to the notion that, as with physical safety, 100% digital safety is unattainable. In addition to prevention, mitigation and recovery must therefore be central in any digital safety policy. The Minister of the Interior and Kingdom Relations indicated the importance of this change of perspective in her letter dated 14 March 2012 concerning the investigations launched following the DigiNotar incident. The Dutch Safety Board is of the opinion that this notion must be implemented in order to structurally improve digital safety at government organisations. Public authorities must take this notion into account in the way they apply digital safety management.

They should not only secure data to the greatest extent possible, but also exercise restraint in collecting and exchanging data. This requires that the negative risks associated with data processing are explicitly weighed at the executive level against the benefits of such processing. In addition, recovery measures must be in place in case data are compromised. These measures must be aimed at restoring the safety of electronic data traffic as quickly as possible and should provide private individuals or companies who suffered damage with an effective solution. Measures of this kind will ensure that private individuals and companies continue to have confidence in the way that the government handles the digital safety of the data obtained from private individuals and companies.

One important lesson that can be learned from the DigiNotar incident is that the safety of digital certificates is undermined when the parties involved retreat too much to the confines of their formal roles rather than assume joint responsibility for safe digital certificate services. The Dutch Safety Board notes that to learn from incidents, the relevant events must be considered without thinking in terms of blame. Only a neutral approach can enable dialogue between the parties involved based on the shared goal of improving digital safety within the government.

Closing thoughts: responsibility in a complex administrative landscape

In the foregoing the Dutch Safety Board stressed the importance of administrative involvement in safeguarding digital safety. However, does not the complex structure of the public sector in the Netherlands contribute as well to the inability of public executives to assume responsibility? Phenomena such as the partial outsourcing and pooling of services may abate the control that public executives can exercise over them, and thereby the extent to which they can really be responsible for them. When control is fragmented, responsibility will be difficult to assign. The Dutch Safety Board does not mean to imply that outsourcing is necessarily bad. On the contrary, organisations can benefit when they join forces and jointly perform certain duties. Especially when 'bulk processes' with few degrees of freedom are concerned, a joint approach makes it possible to achieve substantial efficiency and quality gains.

That said, the Dutch Safety Board believes that it is important for organisations in the public sector to explicitly consider the question as to how and by whom administrative responsibility should be assumed, prior to effecting drastic changes in terms of the allocation of duties. Taking this step will ensure that the responsible authority can fulfil his or her responsibility in full.

RECOMMENDATIONS

Based on the investigation, the Dutch Safety Board makes the following recommendations.

To the Minister of the Interior and Kingdom Relations

1. **Ensure that administrators of all public authorities assume full responsibility for controlling digital safety.**

To this end, develop a programme that communicates to administrators of government organisations the importance of digital safety and provides them with the understanding and skills required to actively manage digital safety in their organisations.

In addition, oblige public authorities to account for the way in which they safeguard digital safety. For this purpose, entrench in the planning and control cycle of public authorities a clearly described public obligation to account for digital safety management, and oblige their administrators to issue an annual in control statement concerning digital safety.

To the Minister of the Interior and Kingdom Relations and the Minister of Security and Justice

2. **Create conditions which ensure that public authorities systematically control their digital safety.**

To this end, ensure that all public authorities comply with the open NEN-ISO/IEC 27001 and 27002 standards, which together provide a framework for systematically safeguarding digital safety. For this purpose, draw up a plan that specifies concrete objectives, measures and a time frame. In addition, designate an organisation that assists public authorities in establishing adequate digital safety.

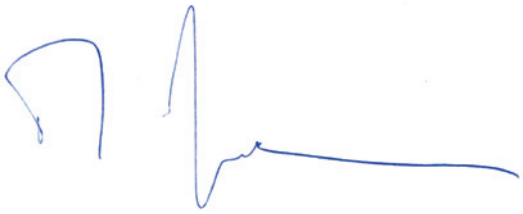
As part of such a systematic approach, municipal authorities, safety regions and the central government should give attention to being prepared for and repairing damage resulting from digital incidents. A single notice by individuals and companies whose data have been affected by a digital safety incident should suffice for adequate measures to be taken by all public authorities involved.

To the Minister of the Interior and Kingdom Relations and the Minister of Economic Affairs, Agriculture and Innovation

3. Ensure that digital certificates are issued and used more safely.

To this end, adjust the roles of OPTA and Logius to ensure that compliance with current regulations governing qualified and PKIoverheid certificates on the part of certificate service providers is actually supervised and enforced.

In addition, foster a change of culture at all parties involved in providing services concerning digital certificates, particularly with respect to reporting and learning from incidents. Make use of safety event reporting practices from other sectors.



T.H.J. Joustra, LLM
Chairman of the Dutch Safety Board

M. Visser, LLM
General Secretary

CONCLUSIONS

The Dutch Safety Board's investigation into digital safety following the DigiNotar incident focused on public authorities. Public authorities are responsible for the data they process. They should handle this data with the utmost care. Even when government organisations contract duties out to external parties, they still bear final responsibility for the safety of data in their possession. They should therefore work towards maintaining the greatest possible grip on the safety of this data and the reliability of electronic data traffic. This starting point is the reason that the conclusions and recommendations based on the Dutch Safety Board's investigation are directed at public authorities.

The central question of this investigation was how public authorities deal with digital safety in administrative and organisational terms, and what problems public executives encounter in this regard. To answer the question, both the DigiNotar incident and the way in which the safety of digital certificates is safeguarded in general were investigated. In addition, a number of public authorities were investigated to explore how digital safety in the public sector is generally safeguarded. Based on the investigation, the Dutch Safety Board draws the following conclusions.

The DigiNotar Incident

Prior to the hacking of DigiNotar, the parties involved verified insufficiently whether DigiNotar operated safely. Both OPTA, responsible for public oversight of part of the company's services, and Logius, the agency that contracted DigiNotar to supply PKIoverheid certificates, were unaware of the actual reliability of DigiNotar's services. Both organisations largely relied on the audits carried out by an auditor that the company had contracted. Working in accordance with regulation, the auditor had indicated that the DigiNotar management system complied with the applicable standards. However, the issue as to whether the company's certificate services actually complied with the applicable rules was checked only to a limited extent.

None of the parties involved were prepared for the DigiNotar incident. No provisions had been made for the event of all certificates, and therefore the certificate service provider itself, being compromised. None of the parties involved had considered the severe repercussions of retracting all certificates issued by a compromised certificate service provider. No-one had realised that this action could cause important data flows with and between government organisations to be interrupted or even ceased, which in turn could cause considerable social disruption.

The safety of digital certificates services and the use of digital certificates

Properly used, reliable digital certificates are essential to the safety of electronic data traffic. The Dutch Safety Board concludes, however, that there is cause for concern in terms of both the proper use of certificates by public authorities and the way their reliability is safeguarded.

Public authorities generally leave the purchasing of digital certificates to ICT departments. This introduces the risk that the level of protection offered by the certificates purchased is not in accordance with the nature of the data they are meant to protect. In this context, many public authorities do not consider themselves capable of independently assessing the reliability of the certificates that they purchase. They instead rely on the expertise of others, as reflected by a quality mark such as WebTrust. Alternatively, they use PKIoverheid certificates that have been 'approved' by the national government.

The limited capability of public authorities to assess for themselves the reliability of digital certificates, makes it all the more important for their reliance on quality marks or PKIoverheid and similar instruments to be justified. The Dutch Safety Board concludes, however, that this is currently the case only to a limited extent.

Neither PKIoverheid nor the system for issuing qualified certificates provide the added value intended by the central government because actual compliance with current regulations on the part of participating certificate service providers is not adequately supervised.

This is due in part to the regulations that govern PKIoverheid. More importantly, the government parties involved, particularly Logius and to a lesser extent OPTA, failed to undertake an effort sufficient to verify the actual reliability of certificate service providers. They based their opinions largely on audits, but those were not primarily aimed at determining whether certificate service providers acted in compliance with the rules applicable to them.

The Dutch Safety Board concludes that PKIoverheid currently does not provide the added value intended by the central government relative to other digital certificates. Due to the design of PKIoverheid and the way that parties involved operate, it offers little assurance that its certificates are actually more reliable than other kinds. Moreover, PKIoverheid often does not seem to meet the needs of public authorities, which consequently make only limited use of the system. Given the critical function of digital certificates in securing electronic data traffic with and between public authorities , the Dutch Safety Board considers this situation unacceptable.

Logius as administrator of PKIoverheid
The Dutch Safety Board concludes that Logius is not fulfilling its role as administrator of PKIoverheid in a way that ensures the intended added value of PKIoverheid certificates relative to other digital certificates being achieved.

In particular, this concerns the way in which Logius supervises compliance with the terms of the contract agreed between the Dutch state and certificate service providers participating in PKIoverheid. Logius is the other party in these contracts on behalf of the Dutch state and should therefore attach importance to strict compliance with the contract terms referred to. Logius verifies only to a very limited extent whether a certificate service provider meets the terms of the contract. The agency takes the position that it can base its supervision largely on the audits that a certificate service provider is obliged to have performed under the terms of the contract.

Logius marginalises its own role by qualifying itself as a 'tertiary supervisor'. The Dutch Safety Board opines that the organisation fails to perform its duties properly by doing so. Precisely because the admission of certificate service providers to PKIoverheid is based on a contractual relationship, Logius, as the other party in this contract, has a strong position to ensure compliance with the contract terms. Given the importance that the central government attaches to PKIoverheid, Logius must make sure for itself that a certificate service provider acts in accordance with PKIoverheid rules, rather than relying largely on the opinion of the auditor.

OPTA as the public supervisor of suppliers of qualified certificates
OPTA is responsible for public oversight of the qualified certificates market. Registration with OPTA is compulsory for certificate service providers wishing to participate in PKIoverheid.

The Dutch Safety Board concludes that OPTA views its own capacity to supervise and enforce the regulations applicable to the supply of qualified certificates as limited. The Dutch Telecommunications Act obliges OPTA to presume compliance with regulations if a certificate service provider can produce a TTP.NL-certificate. Inclusion of this legal presumption in the Act effectively restricts OPTA's powers to supervise. As a result, OPTA fulfils its supervisory role only to a limited extent.

Their difficult position notwithstanding, the Dutch Safety Board is of the opinion that OPTA retreats into a marginal role too easily. The Dutch Safety Board expects a public supervisor to be more vocal and assertive when prevailing legislation and regulations make the effective performance of its duties impossible. A supervisor should push the limits of its authority if he considers doing so necessary for the proper functioning of the sector in which he operates. In this regard, the Dutch opines that the legal presumption included in the Dutch Telecommunications Act does not prohibit OPTA from determining through investigations of its own whether registered certificate service providers do in fact comply with legal requirements.

Government organisations and digital safety

Safeguarding digital safety

The Dutch Safety Board's investigation revealed major differences in the way that individual government organisations fulfil their responsibility manage digital safety. The Dutch Safety Board identified two factors in particular that seem to promote a systematic approach to digital safety. First, organisations where data processing belongs to the primary process seem to apply more stringent digital safety management than organisations where data processing is considered to be merely a means to achieve other organisational objectives. The Social Insurance Bank and the Tax and Customs Administration are examples of organisations at which data processing is part of the primary process. Second, digital safety seems to be better safeguarded in processes to which specific regulations apply (e.g., the municipal records database or the work and income chain) than in processes in which such regulations are absent.

Nevertheless, the Dutch Safety Board does not necessarily advocate that data processing by public authorities be regulated by stricter laws. It believes that such an approach would not sustainably improve digital safety because it would fail to address the responsibility of public authorities themselves. The Dutch Safety Board believes that public authorities must themselves formulate a course of action to safeguard digital safety, in a way appropriate to the specific contexts in which they operate.

The Dutch Safety Board has the impression that many government organisations do not take into account the sensitivity of the different types of data that they process in their digital safety management. These organisations also do not seem to identify and list the threats to this data. In the opinion of the Dutch Safety Board, such an approach would be necessary to arrive at a motivated decision as to the way in which data should be secured and the way in which the safety required can best be organised.

In general, it seems that many public authorities tend to leave digital safety entirely to ICT experts. In such cases, governance of digital safety is frequently inadequate. Administrators and senior management are often not capable of asking the right questions. Because they lack knowledge of and insight into the subject matter, they fail to adequately safeguard digital safety in administrative and organisational terms. Crucial administrative decisions about digital safety policy and risk control are at present usually made by ICT department members of staff rather than by the individuals who bear administrative responsibility. Sufficient awareness of and insight into threats to digital safety is therefore often lacking at administrative level. Recent events such as the DigiNotar incident have cast this inability to administratively direct digital safety in bold relief. Nevertheless, although the vulnerability of digital safety is now far more apparent, it seems that many government organisations have not yet found a way of translating the concomitant sense of urgency into concrete perspectives for action. Several recommendations set out in this report address this problem.

Current legislation and regulations, sector standards and contracts provide open standards for digital safety. Open standards are necessary in the rapidly changing digital world. The investigation revealed, however, that it is difficult for government organisations to keep pace and adapt in this context. Administrative involvement, clear direction, explicit control and supervision and sufficient knowledge is required for the purpose.

The highly digitalised Dutch government is strongly dependent on the functioning of ICT systems. The interrelatedness of these systems requires an overall view and a degree of direction that are currently lacking. The DigiNotar incident showed that a digital government is vulnerable in terms of both the data of private individuals and companies that it processes and the failure of vital infrastructure such as ICT systems as a result of disruptions. These new vulnerabilities are such that the government must direct the way in which they are controlled.

The central government as the party responsible for the overall system
The Dutch Safety Board is of the opinion that the central government has a system responsibility for digital safety in public authorities. This responsibility entails that the central government must set enabling conditions that make it possible for individual government organisations to assume their own responsibility for digital safety. In the Dutch Safety Board's view, this system responsibility applies to the entire public sector. It could even be asserted that it applies to society as whole, seen that parties in the private sector can also pose a serious threat to the public interest if they do not adequately safeguard digital safety.

The central government currently exercises its system responsibility by according a coordinating power for the provision of information within the civil service to the Minister of Interior and Kingdom Relations. In addition, the central government considers it its duty to promote digital safety also outside the civil service.

Based on its investigation, the Dutch Safety Board concludes that it would be desirable for the central government to lend shape to its system responsibility for digital safety more vigorously. By making more active use of its regulatory power and central position in public administration, the central government can promote the improvement of digital safety by all public authorities, yet without adversely affecting the autonomy of local and regional authorities and autonomous administrative authorities. Various recommendations set out in this report address this aspect.

The Dutch Safety Board

telephone +31(0)70 333 70 00 • **e-mail** info@safetyboard.nl • **website** www.safetyboard.nl

visiting address Anna van Saksenlaan 50 • 2593 HT The Hague

postal address PO Box 95404 • 2509 CK The Hague • The Netherlands