1 Management summary

At the time of writing this report, organisations in the critical sectors (energy, gas, water, distribution, flood defence etc.) in the Netherlands and Western Europe have not yet encountered any major problems affecting IACS (Industrial Automation Control Systems) as a result of a cyber attack. In other, non-critical sectors and outside Western Europe, however, there have been various examples of disruption to IACS systems and the associated means of production.

Since a cyber attack on IACS systems can lead to incidents with major impacts, it is necessary for the government to oversee IACS security within the critical sectors. In addition to its monitoring duty, the government has a duty to provide information – including with regard to the risk of attack by state actors.

In consultation with the client (the Cyber Security Council), the categories established by the NCTV have been used[1] for the purpose of selecting the sectors considered to comprise critical national infrastructure within the scope of this research. As the present research focuses on IACS systems, the sectors in which such systems are of above-average importance have been included as well.

The present research demonstrates that organisations in the critical sectors have identified the potential IACS-related (legacy) problems and have taken measures to mitigate any risks to the furthest possible extent. This does not mean, however, that there is nothing more to be done. Not all organisations in the critical sectors have as yet fully implemented the planned initiatives for improvement. Strategic guidelines have been set out within the organisations in the critical sectors and the CISOs (or their counterparts) indicate that sufficient funds will be made available to mitigate the risks. The research results also demonstrate that it remains vital to conduct national and international drills and prepare for potential attacks.

While it is true that a high-impact IACS incident has yet to occur, this does not mean that no problem areas exist or that new measures would not be useful and necessary. The most significant issues and opportunities for improvement as identified in the present report exist in regard to:

- **Improving cooperation within each of the sectors:** This can be realised by drafting a joint sector-specific IACS security framework (either with or without the help of the supervisory body), encouraging and facilitating ISACs (Information Sharing and Analysis Centres) and cooperating to organise drills of sector-specific IACS attack scenarios, both nationally and internationally.
- **Enhancing the exchange of information:** When a limited number of security officials within companies in the critical sectors have been granted sufficient security clearance, it is easier for parties such as the AIVD (General Intelligence and Security Service) to share confidential information regarding threats.
- **Applying standard contractual clauses:** Not all current IACS contracts (within the critical sectors) sufficiently require suppliers (and subcontractors) to safeguard the long-term security of their IACS systems.
- **Enabling exceptions in the tender process:** At this time, it is not possible to exclude a party from a tender based solely on the advice of the Ministry of Justice and Security. Explore whether this can be resolved by establishing an exceptional provision for the critical sectors.

[1] https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

From the literature review and on the basis of the interviews conducted, it was determined that no major policy adjustments are required to preserve the security of the critical sectors. What *is* needed, however, is continued attention to the timely implementation of planned operational measures to improve IACS systems. Additionally, by introducing a number of improvements (see above and section 8) it is possible to further enhance the digital resilience of the critical sectors.