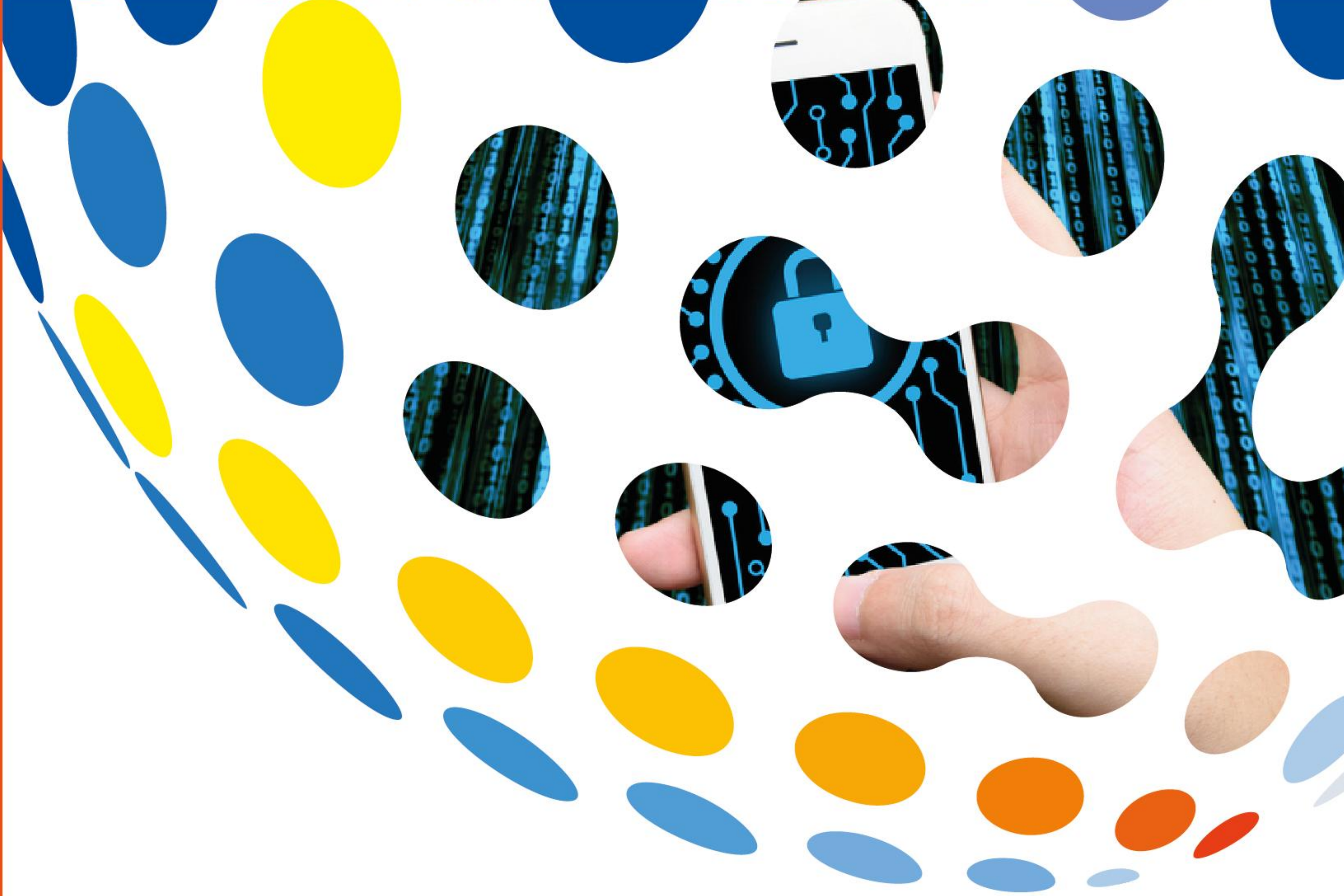

EU Coordinated Risk Assessment

Detection Equipment

30 January 2026

NIS COOPERATION GROUP

Executive summary

This is a coordinated Union level security risk assessment of detection equipment used by EU law enforcement and security operators at EU border crossing points, carried out under Article 22 of the NIS2 Directive by the Network and Information Systems (NIS) Cooperation Group in cooperation with the European Commission and ENISA. The primary objective of this report is to provide a comprehensive overview of the cybersecurity risks and their consequences, as mitigating measures which are considered necessary to efficiently address them, whether in a context of stand-alone use of the equipment or in an interconnected and interoperable environment. This would ultimately pave the way towards a common and coherent EU approach to detection equipment security.

Detection equipment comes with new and significant cybersecurity risks as it is broadly considered as part of the EU critical infrastructure, particularly when connected to sensitive EU systems and networks. Compromised detection equipment can be controlled remotely, exploited as an attack vector or neutralised to support malicious acts. Incidents can also result from human error, system failures or natural phenomena. All these risks raise serious concerns for the EU security, the safety of its citizens and its critical infrastructures. In the light of the EU's principle of free movement of goods and people, these risks are inherently cross-border and require Union-wide coordination.

The risk assessment identifies 13 generic risks, based on an all-hazard approach and in relation to the detection equipment supply chains. The risks have been assessed in terms of their impact and likelihood, resulting into a number of substantial risks reflecting the high strategic value of the assets involved for the EU's economic and internal security and the numerous spillover effects affecting other sectors in case of materialisation of the risks. The highest ranked risks are related to the dependency on a single or limited number of manufacturers, authorised (e.g. maintenance) and unauthorised access affecting the performance of the detection equipment and/or the integrity of the sensitive information related to it and malware introduced to jeopardise or distort the information, systems or networks through the equipment.

The evaluation of the risks has been done on the basis of the current level of interconnectivity, meaning that the detection equipment is still mainly operated as stand-alone equipment for the majority of the customs administrations of Member States (both for technical and security considerations), while in major logistics hubs such as ports and airports, the equipment is in a much more advanced integration phase into larger ICT systems. As EU customs move towards an interconnected environment with the creation of the EU Customs Authority and EU Data Hub, the impact of the risks will increase significantly in the context of integration and interoperability of the equipment. This is particularly valid for the risks categories ranked with the highest impact.

EU law enforcement and security operators benefit from detection equipment to ensure security at EU borders (including ports and airports) which needs to be safe and secure and should be subject to strong (cyber)security protective measures. Although every administration adopted mitigating measures related to cybersecurity risks, the main outcome of the assessment highlights a lack of EU common approach both in terms of evaluation of risks and cybersecurity protocols, as well as in terms of assessing and working with high-risk suppliers.

For the effective management of those risks, a number of mitigating measures are identified in this assessment. They call, amongst other measures, for the effective application of EU level adequate measures for high-risk suppliers, the procurement practices, including the integration of security aspects and requirements into the tenders, the maintenance practices and the security protocols for the use and access to the equipment. The detection equipment market itself, dominated by a limited number of manufacturers of non-EU origin, has shown severe shortcomings and additional challenges for the EU security, particularly with regard to de-risking measures, securing critical infrastructures, diversification of the market and availability of the equipment (and spare parts).

These elements have an impact both on the security of the equipment and other technical aspects (risk mitigation measures), the future integration in interconnected systems (suppliers assessed as high-risk in certain Member States provide equipment in other Member States who do not share the same evaluation to the same suppliers) and the procurement of equipment.

Disclaimer

The document is legally of non-binding nature. It is only of advisory character and therefore cannot alter the application of cybersecurity measures applicable in Member States. References to terms such as ‘critical supplier’ or ‘high-risk supplier’ should be understood as working concepts for the purpose of creating a common framework. Those are without prejudice to national laws implementing the NIS 2 Directive or sector-specific EU legislation, such as the Digital Operational Resilience Act (DORA).

Table of Contents

1 Introduction

The cybersecurity risks related to detection equipment are a growing concern for the EU's security, particularly when such equipment is used for security screening and controls of goods and persons, at ports, airports and other border crossings. While detection equipment technology offers means to detect concealed items and detect other threats, thus playing a central role in security screening processes, it also presents potential risks related to the cybersecurity, data security, privacy, competitiveness and the overall security of the EU and the safety of its citizens, as the equipment often contains, is involved in or is connected to sensitive information.

Detection equipment, like any technology employing software and internet connection, is vulnerable to cyberattacks, potentially compromising its functionality (detection algorithms in airport screening systems, etc.) or allowing for manipulation/distortion of the information (EU sensitive border controls and trade data, images etc.) and interference with other ICT systems. Detection equipment can also be exposed to vulnerabilities arising from human error, system failure and natural phenomena. Human factors such as improper operation, insufficient maintenance or inadequate training may lead to reduced detection accuracy or complete malfunction. System-related failures, including hardware defects, software bugs or power interruptions, can compromise the reliability and availability of the equipment. In addition, natural phenomena, such as extreme weather conditions, floods, lightning, or seismic events, can physically damage the systems or disrupt their functionality.

While detection equipment is widely available across the hundreds of border crossing points (including ports and airports) and logistics hubs, allowing to control the flow of goods and persons, its interconnectivity varies greatly (e.g. equipment in ports and airports is largely integrated while customs and other border controls systems are rather on the way to achieve a greater and harmonised interoperability/interconnectivity). This integration opens significant vulnerabilities across the various logistics, EU law enforcement and border control data networks and systems, not only in terms of data mining and unauthorized data access, but also by enabling potential remote hostile actions against the ICT infrastructure supporting security management platforms, EU border operations and/or against the performance of the equipment itself[1].

The cybersecurity risks are further amplified by the characteristics of the detection equipment market – a niche market dominated by a limited number of manufacturers of non-EU origin. Most of the companies operating in the market are big players in other relevant sectors such as security, aviation, military, or health where similar technologies are used. The uptake of an EU manufacturer has proven challenging as EU investments in research and development have supported the emergence of startups and technologies, but these were quickly absorbed by the leaders dominating the detection equipment market.

Previous initiatives

In the field of customs, ensuring the security of detection equipment has been one of the primary objectives for the Commission, in particular since the start of the dedicated customs control equipment funding programme – the Customs Control Equipment Instrument (CCEI)[2]. In order to support the security requirements in the CCEI calls, particularly the 2023 call[3], the Commission issued guidance on security[4] and highlighted the concrete actions and specific provisions which Member States have to consider, including their integration in the procurement and purchase procedures in order to guarantee the security requirements. At the same time, the coordinated EU programme of research and innovation investment[5] provides support for developing European autonomous cutting-edge technology in security scanning and detection in general, aiming at mitigating Europe's dependency on foreign solutions and

[1] According to a report by the World Customs Organization (WCO), the global trade community loses billions of dollars annually due to cyber-attacks on customs digital systems World Customs Organization

[2] Regulation (EU) 2021/1077 of the European Parliament and of the Council of 24 June 2021 establishing, as part of the Integrated Border Management Fund, the instrument for financial support for customs control equipment

[3] Ares(2023)8512503-CCEI Programme Call: CCEI-2023-EQUIP-IBA

[4] Ares(2022)4027493-Customs Control Equipment Instrument: Ensuring the security of the equipment funded under the Instrument

[5] DG HOME coordinates, in close cooperation with DG TAXUD, the EU programme of research and innovation investment to develop European autonomous cutting-edge technology in security scanning and detection.

technologies, while the possibility of excluding high-risk suppliers and any entities with foreign government ties has been introduced in Horizon civil security calls[6].

Source problem

Despite all measures and guidance taken so far, international partners and EU authorities[7] have voiced concerns about the cybersecurity of the detection equipment. When purchasing detection equipment, several Member States have identified, through the involvement of their national security authorities, equipment manufacturers posing risks to their national security and essential security interests. These risks can manifest as targeting of individuals, systems and organizations to gather intelligence, exert influence or coerce individuals within organizations to provide access to sensitive information or systems and/or distort the functioning of the equipment and the vital controls it allows to perform. Foreign governments may conduct cyber espionage to gather sensitive information about trade, individuals, or critical infrastructures or obtain strategic information on military efforts. Compromising software or hardware components used in critical systems can allow foreign actors to introduce backdoors or malicious codes or distort the performance of the equipment to facilitate hostile malicious acts. Remote work setups can create new vulnerabilities that foreign actors can exploit to gain access to systems and data.

Divergent opinions and evaluation practices, both in terms of security protocols and for assessing the profile of the manufacturers and their equipment, contribute to a variety of risks which are unevenly addressed across Member States. The use of detection equipment by certain Member States on a stand-alone basis as opposed to those Member States who have integrated the equipment already in larger ICT systems, leads to different security concerns and require various protocols to tackle those

[6] HORIZON-CL3-2025-01-BM-03: Open topic on better customs and supply chain security. HORIZON-CL3-2025-01-SSRI-04: Accelerating uptake through open proposals for advanced SME innovation" includes as objective: "reduce technological dependencies from non-EU suppliers in critical security areas".

[7] In the light of the potential threat to data and cybersecurity impacting technology for the screening of cabin and hold baggage, the United States and Canada have raised a general concern that this transfer of data may covertly share screening information with its foreign HQ that could give a competitive advantage to the manufacturer or reveal security check point vulnerabilities. In 2022, several members of the European Parliament issued a letter challenging a tender to award scanners in Strasbourg Airport due to security concerns.

concerns. These divergences of evaluation methods, opinions and practices generate important variations in the procurement practices and the approaches towards the exclusion of high-risk suppliers from public procurements and, in general, towards the reduction of the dependency of the EU law enforcement/border authorities/security operators on them. Certain Member States exclude specific manufacturers from any public procurements while other face serious challenges (including legal disputes) to exclude them, despite indications or substantiated information regarding potential high risks posed by those manufacturers.

In this respect, Member States had to rely on the assessment of their national security bodies which considered the threats associated with detection equipment directly affected the national security of the Member State[8]. In one Member State the available intelligence and the identified risks due to the suppliers' ties with a third-country foreign government has led the Ministry of Finance of one Member State to exclude that company from a public tender for the purchase of detection equipment for customs controls. This Member State relied on the opinion of the national security agency who concluded that the potential dependency in these sectors on a third-country strong geopolitical actor, which seemed to be increasingly using economic files to achieve its own political objectives[9], inherently poses a security risk to the affected sectors. Although the Member State's detection equipment inventory already had equipment supplied by that particular company, the units in use were not connected to each other or to a central system at that time. However, the Member State initiated the integration of this detection equipment into an advanced overarching network, which led to optimised and comprehensive data management and improved controls. The new detection equipment would have become part of new data network. In that situation, the use of the company's equipment posed a particularly high security risk, associated to the essential security interests of the Member State.

In another Member State, the intelligence agency warned that the active penetration of foreign investments posed the risk of losing control over resources and infrastructure, market distortion, and political influence. The reasons were not further

[8] Discussions with the customs administrations, as well as experience gathered from grant implementation for the purchase of customs control equipment, have shown that there is no common approach in assessing the risks raised by high-risk supplier.

[9] Belgium - Judgment of the State Council n° 256.645 of 31 May 2023.

deployed as they were categorised as highly sensitive information, but the risks of that equipment integrated in critical infrastructure was associated with risks to national security[10].

Furthermore, beyond uneven expertise and information on the matter in Member States, important differences in national laws, practices, technical and evaluation standards exist and continue to increase due to the nature of the detection equipment market leading to fragmented practices. While cybersecurity standards and protocols, where applied appropriately, may be reasonably assumed to protect detection equipment from outside interference and the risks associated with them, there is a lack of common standards, protocols and EU coordinated approach particularly when the equipment is interconnected. Crucially, the likelihood of an attack is assessed higher in the context of interconnectivity or interconnected equipment and where the attacker has either direct access to critical assets during production or through remote access after deployment.

The specific types of antagonistic cyber threats (e.g., malware, ransomware, phishing, insider threats) are prevalent in the environment where the equipment is deployed. The integration of detection equipment into the network infrastructure and larger ICT systems significantly increases the impact and its exposure to threats and the potential for malicious acts by the attackers. In addition, given the cross-border nature of civil aviation, the compromise of detection equipment in a single Member State, particularly when sourced from a high-risk supplier, could generate Union-wide repercussions, including the potential imposition of operational restrictions by international partners on flights or cargo screened with such systems. The growing interconnection of aviation security detection equipment with airport IT infrastructures, operational databases, and security management platforms, combined with the automation of detection processes, amplify the impact of any compromise, as disruptions may directly affect primary screening functions and airport operation continuity.

[10] Source: Reuters - Lithuania blocks Chinese scanning equipment on national security grounds – last accessed on 14 August 2025.

Request for a risk assessment on detection equipment

As outlined in the European Economic Security Strategy[11] a global increase in geopolitical tensions and hostile economic actions, cyber and critical infrastructure attacks, foreign interference, dependency, and market domination have exposed risks and vulnerabilities in our societies, economies and companies. The EU must be better prepared for evolving, new and emerging risks that have arisen in this more challenging geopolitical context. In this context, the security of the EU critical technologies is essential for the functioning of its internal market and its vital societal and economic sectors.

In order to fulfil their mission, EU law enforcement such as customs authorities, border authorities, police and airport/port oversight authorities and managing bodies and other related authorities present at the EU borders, including EU ports and airports (hereinafter the “EU law enforcement”/operators), rely on detection equipment allowing them to perform efficiently the controls needed. The efficiency of the equipment is further reinforced through its interconnectivity (with other systems and also with other relevant authorities) allowing for an efficient exchange of information that ultimately strengthens the analytical capacity of the administrations.

Customs act as the first line of defence when it comes to goods entering the EU internal market, and their contribution to the protection of EU citizens and security is therefore crucial. As such, customs contribute and play a key role in ensuring the integrity and the security of the supply chains. Equally, European borders, port and airport authorities and managing bodies play a crucial role in maintaining security, by preventing unlawful acts that could threaten lives, property, or trade, etc. The EU fosters cooperation between Member States, international organizations, and private sector stakeholders to ensure a high level of security in ports and airports. Effective EU border management ensures the functioning and security of the Schengen Area.

[11] JOIN(2023) 20 final, Joint Communication to the European Parliament, the European Council and the Council on “European Economic Security Strategy”

Member States requested and supported cooperation at EU level in order to agree on a common and coherent approach to the security of detection equipment[12]. The approach should include both technical/quality standards and improved procurement procedures, allowing for recommendations to integrate more effectively security in the public tenders considering the common challenges in Member States. The threats raise serious concerns for the safety and privacy of citizens and critical infrastructures and for national security. In view of the EU's principle of free movement, these risks are inherently cross-border and require Union-wide coordination.

Furthermore, the increasing importance of the military mobility is also dependant on the presence of secure and performant detection equipment. The swift and seamless movement of military personnel, materiel and assets, are critical for the European security, with recent EU initiatives focusing on removing regulatory barriers for military movement, upgrading transport infrastructure, and investing in dual-use technology like scanners to detect illicit items and speed up legitimate trade. Military mobility must benefit from secrecy because maintaining information security protects against enemy intelligence gathering and operational disruption, which is crucial for swift, decisive movement and supply chain integrity. Where detection equipment is essential for security, data acquisition, and logistics, their control processes, whether physical, digital, or environmental, they should be secure enough so that the risks associated with it does not impact the speed and flexibility of military movement.

Last but not least, in terms of timing, the risk assessment is also necessary in the context of the ongoing Customs Reform[13], which envisages the establishment of a new EU Customs Authority and Data Hub, where efforts are made to create interconnected, digital systems and processes that allow customs and non-customs authorities, as well as economic operators, to seamlessly share and access information. This improves efficiency by providing a single interface for data submission (the EU Customs Data

[12] This is also supported by the Commission's initiative to develop EU Voluntary Detection Equipment Standards (outside the aviation sector). The initiative aims to set clear operational and technical boundaries to prevent unauthorized data harvesting or other forms of illicit access. Voluntary EU requirements for oversize x-ray equipment widely used in customs and border controls will address current vulnerabilities highlighted by the risk scenarios listed in the report.

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0258&qid=1684913361276Proposal for a Regulation of the European Parliament and of the Council establishing the Union Customs Code and the European Union Customs Authority, and repealing Regulation (EU) No 952/2013

Hub), enables real-time, EU-wide risk management through data pooling and analysis, and ensures a harmonized, less burdensome approach for businesses by reducing redundant data submissions across multiple national and Union systems. In this context, the security of the equipment integrated in this system will play a crucial role.

1.1. Legal Context

The risk assessment on detection equipment is a coordinated security risk assessment of detection equipment carried out under Article 22 of the NIS2 Directive[14]. Under this provision, the NIS Cooperation Group, in collaboration with the European Commission and the EU Agency for Cybersecurity (ENISA), may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

Previous coordinated risk assessments have addressed telecommunications and electricity sectors, 5G networks as well as the recently adopted risk assessment on connected and automated vehicles (CAV). They covered technical risks relating to specific components and systems, but also strategic or non-technical risks which relate to high-risk suppliers deemed susceptible for interference by a third country or other criteria. These exercises together with the EU ICT Supply Chain Security Toolbox also provide the basis for this risk assessment.

The risk assessment is in alignment with the main priorities for the Union as set out in the European Internal Security Strategy (ProtectEU)[15] in the field of security, focusing on four strategic priority areas where the Union can bring added value to support Member States in fostering security for all people living in Europe.[16] Provisions laid in various Union acts tackling security and cybersecurity should apply to security requirements related to detection equipment: the NIS 2 Directive, the Directive on the

[14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[15] Supra 10.

[16] I.e. (i) a future-proof security environment; (ii) tackling evolving threats; (iii) protecting Europeans from terrorism and organised crime; and (iv) a strong European security ecosystem.

resilience of critical entities (CER)[17], the Cyber Resilience Act[18], and the Cybersecurity Act[19] establishing the European Agency for Cybersecurity (ENISA).

Additionally, ProtectEU refers directly to the "Resilience of supply chains": Europe must reduce its reliance on third-country technologies, which can lead to dependencies and security risks. The European Commission aims to mitigate dependencies on single foreign suppliers, de-risk the supply chains from high-risk suppliers and secure critical infrastructure, and develop industrial capacity on EU soil, as specified in the Competitiveness Compass[20] and the Clean Industrial Deal[21]. The European Commission promotes an industrial policy for internal security by collaborating with EU industries in key sectors to produce security solutions like detection equipment, biometric technologies, and drones, incorporating security by design features. Equally, by revisiting EU procurement rules, the European Commission will assess whether the security considerations in the 2009 Defence and Security Procurement Directive[22] are sufficient to address law enforcement and critical entity resilience needs.

For the EU law enforcement, the use of advanced technologies such as adequate, safe and secure equipment, artificial intelligence, data analytics tools and risk assessment management systems is needed to identify all potential risks and threats stemming from trade and security at the EU border and design/implement the adequate controls accordingly[23].

[17] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[18] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[19] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[20] COM(2025)final - Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy

[21] Supra 18.

[22] Supra 18.

[23] Article 3(e) of Regulation (EU) 2019/18964 enables EU law enforcement to maximise the impact of the Union and Member States budget through co-sharing and inter-operability of detection equipment. The CCEI Regulation, Article 5(3), provides for coordination mechanism ensuring efficiency and interoperability between all the equipment purchased with the support of Union programmes and

The CCEI specifically provides financial support for Member States to acquire modern and secure customs control equipment[24], with additional security requirements integrated into guidelines[25]. The CCEI grants include provisions for security, data protection, and cybersecurity aspects, guiding Member States on how to address these issues and promotes strongly the interoperability and interconnectivity of the equipment. Cybersecurity for customs control equipment involves incorporating stringent cyber-resilience and data protection requirements into the procurement, design, and daily use of state-of-the-art equipment like detection equipment and detection systems.

The regulatory package relating to the EASA Regulation EU/2014/379, in particular Part IS (Information Security)[26], introduces dedicated obligations for aeronautical operators and suppliers, focusing on the protection of information systems, threat assessment and cyber resilience.

In the field of aviation security (AVSEC), mandatory requirements[27] apply to the use of detection equipment, including security scanners, explosive detection systems and automatic prohibited items detection software. The new EU AVSEC baseline[28] further reinforces this technology-driven model by promoting the deployment of cutting-edge equipment with automated threat detection capabilities. Since 2019, cybersecurity requirements have been in place for critical aviation security assets, including detection equipment, to protect civil aviation security ICT systems and data from cyber threats. These measures require that Member States implement cybersecurity controls based

instruments, and therefore its efficient use. Equally recitals 2 and 6 of the Regulation provide for the need of secure equipment and for cyber-security resilience and rules.

[24] Recitals 6 and 7 of the CCEI regulation binds the purchase of customs control equipment to cybersecurity resilience while Article 3(2) of the Regulation sets as an objective for contributing to adequate and equivalent results of customs controls through the transparent purchase, maintenance and upgrade of relevant, state of-the-art, such as secure, safe and environmental-friendly, and reliable customs control equipment, thereby supporting the customs authorities acting as one to protect the interests of the Union.

[25] Supra 6.

[26] Commission Regulation (EU) No 379/2014 of 7 April 2014 amending Commission Regulation (EU) No 965/2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council.

[27] Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security.

[28] According to Commission Staff Working Document (CSWD) of 2 February 2023 'Working towards an enhanced and more resilient aviation security policy: a stocktaking'.

on risk assessments, and mandate background checks for individuals with administrative privileges or unsupervised, unrestricted access to such critical ICT systems and data. Airport operators, air carriers, and relevant entities are required to identify the critical ICT systems and data that could be affected by cyber-attacks impacting aviation security, in accordance with Article 1(7)(2) of Regulation 2019/1583.[29] According to Article 1(7)(3) of this Regulation, measures to protect such critical systems and data from unlawful interference must be clearly defined, developed, and implemented in accordance with a risk assessment carried out by the respective airport operator, air carrier, or entity.

1.2. Structure and Key Characteristics of the Report

This report addresses the key findings on the technical and non-technical cybersecurity risks related to detection equipment and provides for generic recommendations. The report is built around three chapters briefly introduced in this section.

Chapter 1 - Introduction

Chapter 1 provides for a global overview of the context related to detection equipment, the rationale for the assessment from the cybersecurity perspective and the legal context of the risk assessment on detection equipment. The concerns raised by EU law enforcement, security authorities and/operators are consistent with the need to perform the risk assessment particularly with regard to the lack of an EU common approach regarding the evaluation of the risks and the design of the mitigating measures in the current context but also the growing need of integrating the equipment into larger ICT systems. Vectors of vulnerability for control equipment may be a supply chain compromise or breach, threat during installation and daily use/maintenance, non-supervision of the supply chain and lack of security clearance of all actors involved. Under these conditions hostile hardware or software can be implanted during the installation, or during maintenance, reparation or upgrades.

[29] Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures.

Chapter 2 – Risk assessment on detection equipment

Chapter 2 refers to the scope and methodology, and details the identified risks and their assessment in terms of impact and likelihood. Experts from the Member States administrations have agreed on the risks identified and, in general, they all identified the mitigating measures already in place to address those risks and the areas to improved them. However, the context in which these risks are evaluated shows differences when it comes to the use of the equipment (standalone vs integrated) and difficulties in assessing the impact of the threats themselves (some Member States while recognising and sharing the substantiated doubts regarding the materialisation of the risks, agreed on the difficulty to provide evidence related to those risks while others also consider that these risks are not sufficiently addressed particularly when it comes to interconnected systems or spillover effects).

Furthermore, section 2.3 of Chapter 2 provides for a detailed evaluation of each risk. The evaluation of risks is built on the comments provided by the experts in national administrations during the various written consultations and during the workshop held on 30 June 2025 in the framework of the CCEI expert group. The evaluation has revealed shortcomings particularly related to the presence of a common approach in the evaluation of the risks and the equipment suppliers similar to a common approach in terms of (cyber)security protocols and mitigating measures.

Chapter 3 – Mitigating measures and recommendations

Chapter 3 of the report lays down the main conclusions and possible mitigating measures resulting from the risk assessment. The lack of harmonisation in terms of protocols for the use and procurement of the equipment, evaluation methodology and security assessment of the high-risk suppliers, security measures and filters for physical and remote access should prompt the Member States and the EU Commission to intensify their efforts towards a common and unified approach, develop strategies for de-risking its supply chains from high-risk suppliers and secure their critical infrastructures. Cybersecurity rules should be reinforced and should contribute to a smooth integration of detection equipment in larger ICT systems and particularly into the upcoming EU Data Hub.

2 Risk Assessment

2.1 Scope of the Report

The objective of the report is to document the outcome of the risk assessment, designed to reach a common understanding and agreement on the relevant technical and non-technical cybersecurity risks related to detection equipment and their impact at EU-level, to identify and assess the risks related to security and cybersecurity (impact x probability) and corresponding mitigating measures, and, finally, to agree on a common and coherent (regulatory and non-regulatory) approach to detection equipment security, comprising both the use and the purchase of the equipment.

The scope of the risk assessment covers both technical and non-technical aspects. It is built upon extensive available existing information about the main security concerns related to the customs detection equipment. The risk assessment is relevant to all Member States as the equipment is available in the entire EU customs union and all border types (airports, ports, land, postal/e-commerce).

For the purposes of this risk assessment, detection equipment using software and/or interconnected to ICT systems and thus most vulnerable to cybersecurity risks was considered. As laid out in the concept note, these may include (but are not limited to): X-ray for detection purposes (scanners (high/low energy), backscatter, CT etc.), Radiation portal monitors (RPM) (fixed/drive-through), Automatic Number Plate Recognition Systems (ANPRS), airport security detection equipment such as explosive detection systems for cabin baggage (EDSCB), combined with Automatic Prohibited Item Detection System (APIDS), Security Scanners (SSc) and Hold Baggage Screening (HBS) are also in the scope.

Other equipment types, subject to the assessment of the experts, such as Isotope Identification Device (RIID), spectroscopy (Raman, FT-IR, XRF, Ion mobility, MS) and endoscopes also fall in the scope of cybersecurity risks, as new technologies appear on the market.

Innovation and interoperability of the equipment are two aspects that were duly considered in this risk assessment. The interoperability and interconnectedness between equipment and larger ICT systems (for risk management purposes, including machine learning and artificial intelligence), further amplify the potential impact of cybersecurity risks/threats.

To ensure a structured approach, the risk assessment followed the 'EU Methodology for Union-level Cybersecurity Risk Assessments' defined by the Cooperation Group on the basis of best practices and lessons learned from previous similar exercises, namely those related to the telecommunications and electricity sectors and to fifth generation (5G) mobile networks. The method involved several phases. In the first phase, risk identification, Member States involved a wide range of national experts from various sectors to identify the most pertinent risks. In the second phase, risk evaluation, the same experts assigned motivated impact and likelihood categories to the risks collectively identified in the first stage. The third stage, risk analysis, consisted of a workshop with the Cooperation Group delegates and extensive follow-up discussions, which led up to the assessment's conclusions and recommendations. Due to the specific nature of the subject, the assessment was conducted as a collaborative effort between experts of the NIS Cooperation Group, the CCEI expert group and the Aviation Security Regulatory Committee (AVSEC Group).

2.2 Risk identification

The result of the first phase of the risk assessment has led to the identification of 13 generic risk scenarios. The table in figure 1, below, illustrates the risks by order of identification, category and risk scenario description.

Similar to other technologies using advanced software solutions, the detection equipment is using artificial intelligence to enhance its capabilities by analysing vast amounts of data to identify better the threats, anomalies, and specific objects in real-time, while also minimizing false positives. The rapid evolution of artificial intelligence can significantly enhance detection capabilities and the efficiency of customs control procedures. However, artificial intelligence also poses a risk to cyber security. While innovation in customs detection equipment is promising, challenges, particularly those related to artificial intelligence and with affects to both the equipment performance and the data connected to it, are apparent and might merit further consideration which could be a different assessment with dedicated experts mandated to address those risks, as these types of risks fall outside of the scope of the present assessment.

ID scenarios	Category	Risk Scenario
Numerical ID for each risk scenario.	*This column categorises the scenario types*	*Risk definition*
RS_01	Malicious act	**Denial of service:** Attacks on the systems and other resources to reduce/compromise the performance or temporarily/permanently make the equipment unavailable.
RS_02	Malicious act	**Unauthorised access** to sensitive information in systems/networks using the equipment as an 'entry' door to bypass the security mechanisms/protocols (back door risk).
RS_03	Malicious act	**Malware:** Malware being introduced to jeopardise the information in the equipment itself; theft of data, distortion of data, destruction of data, spoofing, exfiltration of data/metadata.
RS_04	Malicious act	**Authorised Access; maintenance/installation**: the activity of equipment installation and maintenance (remote and physical) provides an exposed risk for intervention on the equipment and materialisation of other risks linked to the data integrity of the systems and/or the performance of the equipment itself.
RS_05	Malicious act	**Unauthorised Access; physical intervention**: the intervention on the equipment and premises by accessing them without authorisation which can result into the materialisation of other risks linked to the data integrity of the systems and/or the performance of the equipment itself.
RS_06	Malicious act	**Unauthorised monitoring of activities:** surveillance of systems and premises through physical and digital means.

RS_07	Human error	**Untrained staff** operate the equipment wrongly causing reduced performance or temporarily / permanently making the equipment unavailable.
RS_08	Other	**Lack of access control** to the equipment or safety/security perimeter (physical and digital).
RS_09	System failure	The equipment and systems have **technical failures** such as failing hardware, faulty updates or unexpected errors which reduces the performance or temporarily/permanently makes the equipment unavailable.
RS_10	Natural phenomenon	The equipment and systems have technical failures or reduced performance or temporarily / permanently unavailable due to **natural phenomenon.**
RS_11	Other	**Dependency/ mono dependency** on single manufacturer or limited number of manufacturers
RS_12	System failure	Technical failure in a **connected system/network** reduces performance or temporarily/permanently makes equipment unavailable
RS_13	Other	**Equipment variations:** Multiple hardware and software versions available within the equipment inventory that cause different and/or unpredictable performance and undetected vulnerabilities.

2.1.1. Key Concepts and Considerations for the Risk Assessments

Key concepts

The risks identified are generic risk scenarios considered as the most relevant and serious for detection equipment. The assessment of their likelihood, considering the challenges in gathering objective evidence for the materialisations of the risks, was evaluated mostly in the light of the mitigating measures already in place considering the specificities of the geopolitical context. In this respect, the use of the equipment as standalone was considered to be one of the most effective mitigating measures, but, while the experts agreed that such measure greatly reduces the detection performance of the various controls via the equipment, the impact of the risks considerably increases in an interconnected environment. Specifically, in the customs environment, the equipment was, at the time of this report, predominantly used as standalone but preparing for greater integration for the vast majority of the customs administrations, while in airport environments, it is generally the larger airports (with higher passenger/baggage throughput and more screening lanes) that already opted to interconnect equipment. This is primarily to enable centralised management of configurations, maintenance, and real-time operational monitoring.

The assessment of the risks in Section 3.2 of the report, shows the likelihood of the risks to be low. Additionally, the likelihood has been considered as low for the vast majority of the risks. It is the lack of harmonised protocols for the impact of the risks that was the highest concern of the experts, particularly in an interconnected environment.

During discussions regarding equipment purchased with EU funds, experts highlighted difficulties to limit participation of high-risk suppliers to the procurements processes. The procurement of the equipment has proven to be particularly challenging and inefficient for the EU customs administrations. The length of the procedures causes uncertainty as to the scheduling of the date of equipment purchase and delivery affecting ultimately the use of the equipment and the performance of the customs and other controls. Furthermore, procurement procedures differ between Member States with regard to the timing and procedures, the rules and conditions applicable to the procedures, particularly in terms of selection and award criteria, and equally with regard to the integration of the security requirements in the tendering documentation. The provision of standardised equipment tender specifications has also appeared challenging due to diverging national procurement procedural and legal specificities despite the guidance developed by the Commission together with the CCEI Expert Group and prominent expert teams, such as CELBET[30].

Key definitions

For the purpose of the report the following considerations have been agreed upon for the assessment of the risks.

- **Detection equipment:** Detection equipment defines devices or systems, used by the EU law enforcement/security operators designed to identify and locate specific objects, substances, or conditions, often for security, safety, or quality control purposes, providing for a way to identify and locate illegal objects/substances that might otherwise go unnoticed, playing a crucial role in maintaining security, safety, and quality in specifically determined environments
- **Strategic value of assets:** The strategic value of the assets involved is an underlying concept for assessing the impact of the risks. Experts agreed that the term "critical assets" covers several key aspects such as people, information, data, including the physical and digital objects and any related resources needed to perform the law enforcement/customs controls. The strategic value of the data has been highlighted as it comprises data on the way the EU performs the customs controls to other valuable trade and security information. Data covered by the term "critical assets" may, according to security internal architecture of each Member State, be considered as sensitive/classified information but this aspect is not harmonised.
- **Spillover effects:** The spillover effects following the materialisation of the risks is the second key consideration and underlying concept for assessing the impact of the risks. Spillover effects due to cybersecurity incidents refer to the negative consequences that extend beyond the directly targeted organization or sector and impact other entities, authorities or sectors. For example, the

[30] Customs Eastern and South-Eastern Land Border Expert Team (CELBET) formed of 11 EU Member States: Finland, Estonia, Latvia, Lithuania, Poland, Hungary, Slovakia, Croatia, Romania, Bulgaria and Greece.

materialisation of the risks in the customs sector might also affect criminal investigations, joint operations with police and other law enforcement authorities, transport, commercial and trade operators, market surveillance authorities, international agreements and relations etc. resulting into a much wider societal harm.

- **Cybersecurity risk:** The potential for loss of confidentiality, integrity, or availability of information systems due to threats and vulnerabilities, leading to adverse impacts on individuals and organizations.
- **Maintenance:** The preventive, corrective and predictive interventions, including operational and functional checks, servicing, repair and overhaul of a piece of customs control equipment necessary in order for it to retain, or to be restored to, its specified operable condition with a view to it achieving its maximum useful life, but excluding any upgrading.
- **Mono dependency:** A mono dependency exists when multiple organisations, either within a specific sector or across society, have a dependency on the same service. The systemic risk created by depending on a single vendor, technology, or architecture can have a widespread impact. If a vulnerability is found in that single component or provider, a large number of systems and applications become vulnerable simultaneously, which can lead to a major security incident.

2.2. Risk Scenarios

The analysis of each of the 13 risks is based on the comments provided by the experts in national administrations. The risks are presented in decreasing order starting with the risk scenario with the highest risk score (impact x likelihood) to the risk scenario with the lowest score, based on the experts' discussions and consensus.

Risk Scenario RS_11
Dependency/overdependency on single manufacturer or limited number of manufacturers

Over-reliance on a single manufacturer or a limited number of manufacturers can create significant vulnerabilities in several aspects. There was a consensus amongst experts that this risk represented the risk with the most substantial impact, combined with an increased likelihood considering the specificities of the equipment market in the EU, the perspective of suppliers' limitations and the identification of high-risk suppliers. Detection equipment is vital for the efficient controls of EU law enforcement and a limited detection equipment market make de-risking strategies very difficult. This dependency can lead to supply chain disruptions, price increases or variations, reduced performance and innovation if the supplier experiences issues or shifts priorities, or even, due to the lack of diversity, being obliged to choose equipment from suppliers with suspicion or danger of third country influence. Diversifying suppliers and fostering stronger relationships with multiple sources are crucial strategies to mitigate these risks, in particular combined with the development of internal expertise (at EU and Member States level). Detection equipment requires other support activities to be put in place and dependency on single manufacturer or limited numbers of manufacturers seriously impacts the flexibility and quality of processes that the equipment is involved in. The impact of dependency on single or limited number of manufacturers has been assessed as substantial and generally considered as affecting and increasing the likelihood and impact of all other risks identified. This dependency was assessed as particularly relevant in the evaluation of RS_09 (technical failures) and RS_04 (maintenance), where the equipment and systems can be affected by technical failures such as failing hardware, faulty updates or unexpected errors reducing the performance or considerably temporarily/permanently impacting the availability and functionality of the equipment.

Purchase of detection equipment is subject to availability on the market. Data gathered from experts and from national administration in the framework of the CCEI grants, highlighted an important number of cases where the purchase of detection equipment suffered important delays due to unavailability of the equipment on the market, both related to hardware and software. The competition in the tenders and the choices/options available to the buyer are often severely reduced.

Purchase and maintenance of the equipment, particularly in the field of customs, are subject to individually negotiated contracts, regulated by national provisions in force. As such, they vary across Member States, laying down different conditions for maintenance and cost related aspects for maintenance, updates and any other technical or non-technical aspects. Equally, and as already stated in this report, there is a lack of common approach on suppliers' security protocols and mitigating actions related to cybersecurity risks. Consequently, equipment suppliers propose and apply different methods for managing cybersecurity risks and certain equipment may present higher vulnerabilities than others. Relying mainly on one vendor for software and hardware can create “vendor lock-in”, limiting the ability to integrate with other systems or switch suppliers in the future. Vendor-supplied software for detection equipment can also have limitations, especially when relying solely on the vendor for monitoring and updates. These may create additional vulnerabilities in particular if combined with inadequate security protocols, lack of robust security measures, or vulnerabilities in the equipment itself. Reliance on one vendor support for updates and maintenance can create a single point of failure, especially if the vendor experiences security incidents. These limitations include incomplete end-to-end process tracking, short data retention periods, lack of intelligent alerting, and potential vendor lock-in. Furthermore, software bundled with hardware may prioritize hardware design over comprehensive observability, and vendor-provided security updates may not always be effective.

Specialized equipment proprietary software, or exclusive service contracts, potentially leading to higher costs, limited flexibility, and reduced bargaining power for the customer, may create a situation of or high dependency on single or limited number of suppliers. Software bundled with hardware may only offer basic status checks rather than in-depth insights into service performance. It may lack features like anomaly detection, service dependency mapping, or root cause analysis, making it difficult to identify the source of problems. Short data retention periods or lack of it, as well as of tracking of access and incidents can lead to the loss of critical information over time, hindering troubleshooting and analysis. Suppliers can potentially introduce malware into their software, which can be difficult to detect and mitigate.

Lastly, thoroughly assessing vendor-supplied software and managing updates can be resource-intensive, especially for administrations with limited staff, time, or budget. Limited availability of spare parts for detection equipment can significantly impact operational uptime and efficiency. This shortage can lead to increased downtime for repairs and hinder preventative maintenance. As technology advances, some parts may become obsolete, making it difficult to find replacements and increasing the risk of equipment failure.

The characteristics of the EU equipment market increase further the likelihood of all these negative scenarios making the risk the highest in terms of impact and probability.

Risk Scenario RS_04
Authorised Access; maintenance/installation: the activity of equipment installation and maintenance (remote and physical) provides an exposed risk for intervention on the equipment and materialisation of other risks linked to the data integrity of the systems and/or the performance of the equipment itself

Authorised access refers mainly to the processes and procedures for granting and managing access to equipment for maintenance and installation tasks, encompassing both remote and physical access. The risk has been evaluated as substantial by national administrations as the activity of maintenance/repair/upgrade is providing an opportunity to access the data and the systems through the equipment and that the access is granted for specific, legitimate purposes like maintenance or installation. This risk scenario increases greatly the likelihood of other risk scenarios assessed with a high impact such as RS_03 (malware) and RS_09 (equipment technical failure) in particular.

Proper access control is crucial (see also RS_08) to prevent unauthorized use, tampering or damaging the equipment, and to maintain the integrity of the systems and data. And while RS_08 has been assessed as unlikely, the same damaging events can occur with a much greater likelihood in the case of authorised access and malicious intent. In addition, experts once again reported that this risk is not addressed according to the same principles and protocols across Member States. The contracts for maintenance are subject to negotiations with the supplier and subject to national contractual rules, along with other national or EU requirements for technical or security aspects. Remote maintenance, which implies an access from a distance and through a network, has been reported as a general practice, with a few exceptions. Some experts equally reported lack of security protocols or clearance for all persons accessing the equipment, whether physical or remote. Lack of access records has been reported by at least one Member State and only a limited number of Member State ensure supervision by habilitated members of national administration when access to the equipment is granted.

Despite divergent protocols applied for maintenance, all experts considered that maintenance is always carried out in accordance with the 4-eye principle (technical specifications require specific profiles for maintenance that should be limited to technical operations without accessing data, different layers of access, data is encryption to further protect the integrity and security of the customs and other systems). However, risks related to malware installed during maintenance process have been considered and the general consensus was that installation and maintenance phases pose high risk for both intentional and accidental compromise.

Risk Scenario RS_03
Malware: Malware being introduced to jeopardise the information in the equipment itself; theft of data, distortion of data, destruction of data, spoofing, exfiltration of data/metadata.

Malware is software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, performance or availability of a system. The threat of malware has been consistently ranked as substantial amongst experts. Malware can be used to steal sensitive information, such as personal details, financial data, trade information, law enforcement controls data, or other confidential information, can alter or corrupt data, making it unusable or misleading, permanently delete or overwrite data, leading to significant data loss.

Malware can be used to impersonate legitimate users or systems, potentially gaining unauthorized access or manipulating information, can secretly transmit stolen data or metadata (information about data) to remote servers controlled by attackers. These actions can have serious consequences, including ransomware attacks, data breaches, and recovery costs can lead to significant financial burden. In general, cyberattacks (malware being a form of such an attack) have become a significant tool in today’s world and cyber issues are geopolitical and have a strong security dimension.

They have become a powerful tool in the hands of state (and non-state) actors and malware had been assessed as a phenomenon with a substantial impact. Aside from the geopolitical dimension, these attacks may be driven by purely criminal intent, such as financial gain, rather than political objectives or national interests, and they can materialise in cybercrimes for financial gain, such as ransomware and phishing scams, as well as threats stemming from human error, insider threats, corporate account takeovers, and the general risk of malware. These attacks can target any organization or individual, regardless of their national origin or political standing, and are often driven by motives like profit, data theft, or system disruption. In addition, potential spillover effects can severely damage the administration's reputation and erode public trust. Traditionally, malware attacks happen at a single point of surface amongst hardware equipment, software pieces or at network level exploiting existing design and implementation vulnerabilities at each layer.

In terms of likelihood, if some experts concluded to a low likelihood of this risk due to the prevailing stand-alone use of the equipment, the general consensus was that suppliers software limitations[31] and possible introduction of malware through a USB key (including during on-site maintenance) can represent realistic scenarios and there is no common approach in terms of mitigating measures in place across Member States.

Risk Scenario RS_09
The equipment and systems have technical failures such as failing hardware, faulty updates or unexpected errors which reduces the performance or temporarily/permanently makes the equipment unavailable

Technical failures can manifest as reduced functionality, system crashes, or complete equipment breakdowns. Detection equipment (x-ray scanners, backscatters, etc) are devices made up of different subsystems (vehicle, generator power supply, many sensors, hydraulics, electric motor movement, hardware and software) which causes occasional interruptions in operation, regardless of adequate maintenance. Components like sensors, processors, or storage devices can degrade over time or experience sudden failures. Software or firmware updates can introduce bugs or conflicts, leading to instability or malfunctions. Unexpected software behaviour, like crashes or freezes, can disrupt operations.

[31] Software limitations have been reported by a Member State where, to prevent malware infiltration AVIRA software cause serious system disruptions and temporary unavailability of the equipment. This limitation has been reported equally by equipment manufacturer which leads to the conclusion that software limitation should be subject to revaluation and mitigating measures standardised.

Extreme temperatures, humidity, or dust can damage equipment and cause failures as well as, sometimes, inconsistent power supply can damage sensitive electronics. Over time, components can wear out and fail, especially in industrial settings. Incorrect configuration, improper maintenance, or accidental damage can also lead to failures.

The general assumption amongst experts is that these risks are mitigated through a well negotiated contract with the supplier, where maintenance and supply of faulty equipment parts is a mandatory part of the contract. However, several experts reported that technical failures may sometimes come with high costs associated to replacement parts or additional maintenance and the most common problem is the dependency on one single manufacturer. For example, a software update, without which the system cannot be upgraded or may result in long time unavailability of the equipment if the manufacturer's software update is not available immediately. As such this risk scenario is volatile and highly dependent on management of the previous three risk categories RS_03, RS_04 and RS_11.

Risk Scenario RS_02
Unauthorized (digital) access to sensitive information in systems/networks using the equipment as an 'entry' door to bypass the security mechanisms/protocols (back door risk).

This risk scenario bears similar characteristics as RS_03 (malware). Although this risk was assessed as substantial, experts considered it as less significant than the previous risks. The reason for this assessment was mainly the prevailing use of the equipment as stand-alone which greatly reduces the likelihood of the materialisation of such risk and becomes a strong mitigating measure. However, the general consensus, particularly confirmed by Member States operating integrated equipment, is that this risk's impact significantly increases in the context of interconnected equipment and interoperability and mitigating measure have to be reassessed specifically to this context. Backdoors in detection equipment pose a significant risk by potentially allowing unauthorized access and control, compromising the integrity and confidentiality of the system. These hidden pathways, whether intentionally placed or inadvertently created, can be exploited by attackers to bypass security measures and steal sensitive data, disrupt operations, or even take control of the equipment.

A backdoor is essentially a hidden entry point into a system or application that bypasses normal security protocols with significant spillover effect. Unauthorized access to system data may allow targeted access to sensitive information, avoidance of inspection protocols, enabling smuggling operations and creating safe corridors for illicit goods. This could harm national and EU security as it undermines enforcement, leads to economic loss, prevents controls on illicit substances with public health consequences, and may trigger political or EU-level response.

Backdoors can be exploited by malicious actors. Risks raised by the manufacturer's updates, particularly through maintenance, appear to be the most difficult to overcome due to the ownership and exclusive control the manufacturers have on the software. In addition, one Member State reported significant challenges in designing and putting in place security measures to prevent the eventuality of a backdoor because the equipment functions as a "black box". Controls enabling detection and prevention of backdoors are very difficult to perform and the only mitigating measure appears to be the limited or inexistent connection to internet access. However, satellite-based connections are inherently more difficult to monitor and control.

In the context of airports, for instance, vulnerability of detection equipment creating backdoors for further attacks and espionage have been reported in relation to the biometric access control systems[32]. Equipment that is connected to airport IT systems, such as Departure Control Systems (DCS), presents a high level of vulnerability. This risk is particularly pronounced when such systems also interface with supporting components, including boarding gate readers, ID scanners, or remote check-in devices. Such connectivity introduces the possibility that not only border control functions, but also customs operations, may be exposed to unauthorized access or manipulation. The vulnerabilities the equipment presents, including remote access capabilities and insecure protocols, can lead to data breaches, unauthorized access, and potential network infiltration. Specifically, attackers can exploit these weaknesses to steal biometric data, manipulate user databases, and even use the devices as

[32] The ongoing evaluation of these scanners has been provided by experts involved in the internal security and home affairs. At the time of this report, the outcome of the assessment of these vulnerabilities for this type of equipment was still under evaluation. https://covertaccessteam.substack.com/p/vulnerabilities-in-zkteco-biometric last consulted on 28 August 2025.

backdoors to compromise enterprise networks. The system allows for remote access for tasks like user data management and photo uploads. An insecure proprietary protocol can expose personal data, including biometric information. Attackers can manipulate the system to add or remove users, potentially granting access to restricted areas. Vulnerabilities in firmware updates and command processing can allow attackers to execute arbitrary code, creating backdoors for further attacks and espionage ([33]).

Amongst the most common measures already in place for already interconnected equipment, experts have reported firewalls, acting as barriers, blocking unauthorized access to network and provide for regular network updates and strong configuration. Network monitoring for suspicious activities as well as network segmentation can limit the impact of a successful backdoor attack by preventing it from spreading to other parts of the network.

Another common source of unauthorized access is insider threats, originating from within the organization. Insider threats can be intentional or unintentional. An intentional insider threat occurs when an individual with legitimate access deliberately misuses it to harm the organization by accessing systems to which he does not have access in principle. This could be for reasons such as espionage, personal gain, or revenge. An unintentional insider threat, on the other hand, occurs when an individual inadvertently causes a security breach, often through negligence or lack of awareness.

Risk Scenario RS_06
Unauthorised monitoring of activities: surveillance of systems and premises through physical and digital means.

Physical unauthorized access/surveillance involves gaining physical entry to a secured area without proper authorization. Digital unauthorized access means gaining access to computer systems, networks, or data without permission through digital means. Unauthorized access can lead to data breaches, compromising sensitive information and potentially causing significant financial and reputational damage.

Additionally, customs and other law enforcement control operations are usually carried out in public spaces - both in ports and airports, controls are carried out in the presence of third parties (dock workers, passengers, etc.). Incidents occurred where criminal organizations were observing customs premises, and two situations were reported where intrusion was established. In those cases, unauthorised surveillance of systems and premises aimed the recovery of seized drugs. The likelihood of such risk scenario was assessed as relatively low due the effectiveness of the mitigating measures that are already put in place (surveillance cameras, firewalls, security screenings and protocols etc.).

Risk Scenario RS_05
Unauthorised Access; physical intervention: the intervention on the equipment and premises by accessing them without authorisation which can result into the materialisation of other risks linked to the data integrity of the systems and/or the performance of the equipment itself.

This risk scenario bears the same impact as RS_04 (authorised access) but has been assessed with a significantly lower likelihood as the effectiveness of the mitigating measures (security and access controls protocols and tools) is greater. Its context is also similar to RS_08 (lack of access controls) described below.

Risk Scenario RS_08
Lack of access control to the equipment or safety/security perimeter (physical and digital)

Unauthorized access, mostly by physical intervention and lack of access control to the equipment, both physical and digital, has been assessed as having similar or same impact. Both risks have been evaluated as substantial due to the vulnerabilities that can be exploited, particularly when this equipment is interconnected.

A lack of proper access control to detection equipment and its surrounding security perimeter, both physically and digitally, creates vulnerabilities that can be exploited. This can lead to unauthorized access, data breaches, and potential disruptions to operations. Unauthorised access to equipment and premises can significantly jeopardize data integrity (the accuracy and consistency of data is not maintained) and system performance. Such breaches can introduce risks like data corruption, errors in data processing, reporting, and decision-making, unauthorized modification, and potential system instability, reduced or compromised performance of the equipment, ultimately impacting operations.

Experts have estimated that the risk is more likely to materialise in environments like ports, where ensuring the security of the control/security perimeter/zone may fail. While most sites have some degree of access control, enforcement is inconsistent, and there are cases of no centralized tracking of authorized personnel. Constant presence of customs or authorised law enforcement officials should guarantee adequate access control. Several layers of access control to the equipment are generally accepted as a satisfactory preventive measure.

Lack of access control and logging greatly increases vulnerability to unauthorised use and tampering. Impact may vary with site security and system complexity. In some Member States national legislation equally pays an important role, imposing a legal requirement that detection equipment should not be left unsupervised and unlocked.

Risk Scenario RS_10
The equipment and systems have technical failures or reduced performance or temporarily/permanently unavailable due to natural phenomenon.

The risks associated to natural phenomenon are mostly influenced by the physical placement of the equipment (different site conditions relate to controls at land borders, ports and airports). Furthermore, the quality and resistance of the equipment guaranteed by the manufacturer for natural phenomenon play an important role. Some of the equipment is not waterproof. Mobile x-ray scanners cannot operate in severe weather conditions: heavy rainfall and snow, strong winds. The NII-systems are parked in garages for customs, police or on military bases. For example, a failure in equipment caused by thunderstorms may occur, and some administrations are exposed to natural hazards, particularly earthquakes and volcanic activity. However, in general, incident records suggest a very low likelihood of occurrence, with a slight exception of heavy rainfalls, overheating, and systems undercooling.

The impact can range from failures, which are temporary and often resolved by simple interventions, to permanent failures that require hardware repair or replacement. Examples include hardware malfunctions, software bugs, or resource overloads. Individual parts of a system can fail, potentially causing a cascade of issues or leading to the system's overall failure. Detection equipment requires a considerable amount of time for availability and / or substitution. This type of equipment is difficult to have redundancy and there is significant time to purchase a substitute.

Risk Scenario RS_01
Denial of service: Attacks on the systems and other resources to reduce/compromise the performance or temporarily/permanently make the equipment unavailable.

Denial of Service (DoS) attack is a deliberate attempt to disrupt the normal functioning of a system or network, preventing legitimate users from accessing its services. Attackers achieve this by overwhelming the target with traffic or requests, causing it to slow down, become unresponsive, or even crash. This disruption can affect various online services. There are physical and cyber vectors (e.g. DoS, ransomware, sabotage) involved. The risk is heightened by outdated systems and weak access controls but it affects also newer systems in case no specific measures are taken. Effects may include delays, loss of service during peak operations, or broader disruption to border processes. DoS would disrupt the logistics chain causing an economic impact. It could also pose a social risk by reducing trust among operators and the public in the reliability of customs. The impact depends on several variables: the internet access restrictions put in place; and the number of affected pieces of equipment and the relevance of each one in the detection process. For example, equivalent equipment at airports of different sizes or scales could have varying degrees of impact.

However, fallback to manual inspection, rerouting and other existing protocols prevent this from becoming a catastrophic scenario. Where the likelihood stands from a theoretical point of view, systems secure networks should provide for sufficient guarantees against this threat. Additionally, for the equipment operated in closed networks, DoS attacks require time to achieve denial which makes DoS attack highly unlikely.

Risk Scenario RS_13
Equipment variations: Multiple hardware and software versions available within the equipment inventory that cause different and/or unpredictable performance and undetected vulnerabilities.

The existence of multiple hardware and software versions within an equipment inventory can lead to performance inconsistencies and security vulnerabilities. Different versions can have varying features and capabilities, leading to unpredictable behaviour and potentially introducing exploitable weaknesses. Older or newer versions might interact poorly, leading to resource contention or instability. It also renders the interoperability and the integration of the equipment into larger networks much more challenging. Integrating devices with different software or firmware can introduce compatibility issues, hindering overall system performance and functionality. Maintaining an accurate inventory and regularly updating systems are crucial for mitigating these risks. Older or newer versions might interact poorly, leading to resource contention or instability. Integrating devices with different software or firmware can introduce compatibility issues, hindering overall system performance and functionality.

This situation renders integrations, support, maintenance and management of the equipment expensive and very complex. A lot of technical limitations will rise and thus difficult to achieve an SLA of the equipment.

X-ray scanners use different file types to save images. While this situation is not ideal, it reflects the current reality—the coexistence of multiple hardware and software components. To improve the accuracy and reliability of the equipment, mechanisms such as double-checking, increasing sample sizes, and other validation methods could be implemented.

Risk Scenario RS_12
Technical failure in a connected system/network reduces performance or temporarily/permanently makes equipment unavailable.

A technical failure in a connected system or network occurs when a component malfunctions, causing a reduction in performance or a complete outage of the affected equipment. This can range from minor disruptions to major breakdowns, impacting functionality and availability.

Experts feedback on this risk revert to the fact that the equipment, particularly for the customs controls is used as a standalone in the vast majority of the Member States administrations. However, experts agreed that although the risk may be amplified in the case of interconnected equipment, the damage to the functionality of the network should not be influenced directly by the technical failure of the equipment particularly as this type of equipment may be disconnected from the network. Nevertheless, just like the assessment of the risk RS_02 also points out, if the technical failure is caused by malware infections, denial-of-service attacks, or unauthorized access, the consequences can be dramatically higher. This type of technical failure of the equipment in interconnected systems can compromise network security and functionality. Malfunctioning routers, switches, cables, or other physical components can interrupt network connectivity. Bugs, errors, or outdated software on network devices can lead to performance degradation or failures. Incorrectly configured network settings or improper handling of equipment can cause connectivity problems or security vulnerabilities. Power outages or fluctuations can also disrupt network devices and services.

Risk Scenario RS_07
Untrained staff operate the equipment wrongly causing reduced performance or temporarily/permanently making the equipment unavailable.

The effectiveness of the detection equipment relies on the expertise of the individuals using it. The evaluation of the impact of the risk found a consensus amongst experts as a moderate impact. A moderate impact of the risk may involve severe consequences for the targeted organisation with some potential spillover effects to other organisations.

Personnel involved in operating the equipment need to be well-prepared and knowledgeable. Equipment and equipment systems require that personnel have different certifications, expertise to prevent data compromise, licence/authorisation to access sensitive functions and data and are provided with specific procedure guidelines to clarify the operative processes and standardize actions, ensuring consistency and reducing the risk of (human) errors. Personnel training should reflect technical aspects of the equipment for smooth operation, safety of the personnel involved (in particularly with regard to the radiation detection equipment), but also cybersecurity rules and limitations of access based on the need to know and level of authorisation.

Staff turnover or complex equipment have been reported as the most challenging aspects with respect to training and experts agreed that the main damage that could incur is mostly related to the hardware and not to software. Lack of adequate training may also be an unintentional insider threat (as referred to in RS_02), occurring when an individual inside the organisation inadvertently causes a security breach, often through negligence or lack of awareness.

In general, as detection equipment requires specific skills for operation and specific requirements for the protection and health of the operators, experts informed that the personnel using the equipment are trained before taking over their functions and constant training is provided to staff. In this respect, experts from sectors which use the equipment as standalone have evaluated the risk as very unlikely to happen due to the rigorous certification/training process and the supervisions already in place for the staff. However, the risk was considered to have a higher impact in the context of interconnectivity and interoperability where layers of accessibility, specific trainings related to cybersecurity rules and access to data as well as security clearance should be re-evaluated.

3 Conclusions

EU law enforcement and security operators benefit from detection equipment to ensure security at EU borders (including ports and airports). The equipment together with the networks and systems to which it is connected bears the characteristics of infrastructure that is critical for the safety and security of the Union and its citizens. As such, the equipment itself and its supply chains needs to be safe and secure, subject to strong protective measures. Designing and deploying such measures across the EU is challenging as the equipment is widely used in a variety of border crossing and logistical hubs (ports, airports, land crossings, postal/e-commerce hubs etc) by various law enforcement and transport authorities. In certain specific cases, like in the case of customs, not all Member States have integrated the equipment into larger national ICT systems. Therefore, the impact and likelihood of the risks identified have been evaluated at a lower level than in the context of integrated equipment or interoperability. However, the assessment of these risks shows that the impact and the spillover effects of the cybersecurity risks increase greatly in the context of integrated equipment. As the EU moves towards an interconnected environment (e.g. the customs reform proposal of the European Commission envisages the creation of an EU Customs Data Hub interconnecting all customs systems and supporting tools), experts agreed that the impact of the risks will increase significantly when the equipment will be interconnected.

Overall, the risk assessment identified 13 risks categories in relation to detection equipment. The risks have been assessed in terms of their impact and likelihood. In terms of impact, the risks range from moderate to substantial, which illustrates the high strategic value of the assets involved for the EU (economic) security and the numerous spillover effects affecting other sectors which could be affected in case of materialisation of the risks. The majority of the risks have been assessed as having substantial impact (consider again the context of predominantly standalone equipment). The highest risk categories are related to the dependency on a single or limited number of manufacturers (Risk RS_11), malware introduced to jeopardise the information (Risk RS_03) and authorised/unauthorised access to sensitive information (Risks RS_04, RS_02). These risks have been already identified as the highest risks categories deserving immediate attention.

In terms of practices and mitigating measures related to the management of the cybersecurity risks, the risk assessment concludes to the following main observations:

a. Customs administrations in Member States deploy different approaches both in terms of the evaluation of risks and the mitigating measures, such as cybersecurity protocols. The management of these risks varies greatly accordingly, providing opportunities for the existence of weak spots that could be possibly exploited by malicious actors (state and non-state).

b. Methods for the evaluation and the assessment of high-risk suppliers also diverge, including in cases when the national security authorities of the Member States are involved in such assessments. This increases the fragmentation across Member States and raises issues particularly in interconnected environments. As a step towards a more effective and efficient approach towards high-risk suppliers, Member States should respect the criteria as laid in the EU ICT Supply Chain Security Toolbox.

c. Equipment maintenance, assessed as a scenario allowing to materialise one of the highest risks in the exercise (theft of data, distortion of data, equipment malfunctions etc.), is performed according to divergent national practices and rules in force and individually negotiated contracts. These allow also the suppliers' remote unsupervised access in a vast number of custom administrations. More importantly, no custom administration within the 27 Member States has developed its own capacity for repair and maintenance, relying solely on the manufacturer and creating a dependency that is detrimental to the EU security (including economic and cybersecurity).

d. Procedures for physical and digital access to the equipment, including staff from all levels and manufacturers' additional staff, also diverge across Member States and in accordance with the use of the equipment, already integrated or standalone.

e. Procurement and purchase processes are also based on divergent national practices, evaluation methods and face various legal limitations in terms of EU and national legislation. Procurement involves a significant administrative burden, leading to delays in the purchase and deployment of equipment and is conducted in a framework making it very difficult to exclude high-risk suppliers based on security grounds.

f. Overall, the detection equipment market with a limited number of manufacturers mainly from non-EU origin is a challenge and risk on its own. Risks to the cybersecurity of ICT supply chains are particularly pronounced in cases where the market is very limited, slowing down de-risking strategies and increasing dependency.

All these divergences create fragmentation in the EU internal market, weaken the security of systems and networks, in turn jeopardizing the Union's security (including economic and cybersecurity) and the one of its citizens as a whole.

4 Recommendations

The below recommendations are non-legally binding proposals and suggestions for improvement identified during the risk assessment process. For efficiency purposes, recommendations cover as much as possible all the risks categories.

The recommendations are relatively generic and create the basis for more specific measures to address the risks identified in the risk assessment.

R.1: Improve the EU resilience and overall cybersecurity posture with regard to detection equipment.

R.2: Cybersecurity – revised and security proof approach to equipment maintenance/repair/upgrade.

R.3: Cybersecurity – develop commonly agreed EU security protocols, including security protocols.

R.4: Supply chain security – effective application of the EU ICT Supply Chain Security Toolbox measures, including for high-risk suppliers.

R.5: Collective situational awareness and sharing of information.

R.6: Public procurement – integrating security aspects in public tenders, more extensive use of joint/centralised procurement.

R.7: Work towards EU technological and digital sovereignty in the area of detection/screening technologies.