COUNCIL OF THE EUROPEAN UNION

Brussels, 26 November 2013 (OR. en)

16493/13

FIN 792

COVER NOTE

From:	Mr Vítor CALDEIRA, President of the European Court of Auditors
date of receipt:	5 November 2013
To:	Mr Linas LINKEVICIUS, President of the Council of the European Union
Subject:	Report on the annual accounts of the European Network and Information Security Agency for the financial year 2012 together with the Agency's replies

Delegations will find attached the European Court of Auditors' report on the annual accounts of the European Network and Information Security Agency for the financial year 2012.

This report is accompanied by the Agency's replies and will shortly be published in the *Official Journal of the European Union*.

Encl.: Report on the annual accounts of the European Network and Information Security Agency for the financial year 2012 together with the Agency's replies.[1]

[1] In English only. The other languages of this report are available on the European Court of Auditors' website: http://eca.europa.eu/.

ЕВРОПЕЙСКА СМЕТНА ПАЛАТА
TRIBUNAL DE CUENTAS EUROPEO
EVROPSKÝ ÚČETNÍ DVŮR
DEN EUROPÆISKE REVISIONSRET
EUROPÄISCHER RECHNUNGSHOF
EUROOPA KONTROLLIKODA
ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ
EUROPEAN COURT OF AUDITORS
COUR DES COMPTES EUROPÉENNE
CÚIRT INIÚCHÓIRÍ NA HEORPA

EUROPSKI REVIZORSKI SUD
CORTE DEI CONTI EUROPEA
EIROPAS REVĪZIJAS PALĀTA
EUROPOS AUDITO RŪMAI

EURÓPAI SZÁMVEVŐSZÉK
IL-QORTI EWROPEA TAL-AWDITURI
EUROPESE REKENKAMER
EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY
TRIBUNAL DE CONTAS EUROPEU
CURTEA DE CONTURI EUROPEANĂ
EURÓPSKY DVOR AUDÍTOROV
EVROPSKO RAČUNSKO SODIŠČE
EUROOPAN TILINTARKASTUSTUOMIOISTUIN
EUROPEISKA REVISIONSRÄTTEN

Report on the annual accounts of the European Network and Information Security Agency for the financial year 2012

together with the Agency's replies

12, RUE ALCIDE DE GASPERI
L - 1615 LUXEMBOURG
TELEPHONE (+352) 43 98 – 1
TELEFAX (+352) 43 93 42
E-MAIL: eca-info@eca.europa.eu
INTERNET: http://eca.europa.eu

INTRODUCTION

1. The European Network and Information Security Agency (hereinafter "the Agency", aka "ENISA"), which is located in Athens and Heraklion[1], was created by Regulation (EC) No 460/2004 of the European Parliament and of the Council[2], amended by Regulation (EC) No 1007/2008[3] and by Regulation (EC) No 580/2011[4]. The Agency's main task is to enhance the Union's capability to prevent and respond to network and information security problems by building on national and Union efforts[5].

INFORMATION IN SUPPORT OF THE STATEMENT OF ASSURANCE

2. The audit approach taken by the Court comprises analytical audit procedures, direct testing of transactions and an assessment of key controls of the Agency's supervisory and control systems. This is supplemented by evidence provided by the work of other auditors (where relevant) and an analysis of management representations.

STATEMENT OF ASSURANCE

3. Pursuant to the provisions of Article 287 of the Treaty on the Functioning of the European Union (TFEU), the Court has audited:

---

[1] Whereas administrative staff remains in Heraklion, operational staff have been relocated to Athens in March 2013.

[2] OJ L 77, 13.3.2004, p. 1.

[3] OJ L 293, 31.10.2008, p. 1.

[4] OJ L 165, 24.6.2011, p. 3.

[5] ***Annex II*** summarises the Agency's competences and activities. It is presented for information purposes.

(a) the annual accounts of the Agency, which comprise the financial statements[6] and the reports on the implementation of the budget[7] for the financial year ended 31 December 2012, and

(b) the legality and regularity of the transactions underlying those accounts.

The management's responsibility

4. In accordance with Articles 33 and 43 of Commission Regulation (EC, Euratom) No 2343/2002[8], the management is responsible for the preparation and fair presentation of the annual accounts of the Agency and the legality and regularity of the underlying transactions:

(a) The management's responsibilities in respect of the Agency's annual accounts include designing, implementing and maintaining an internal control system relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error; selecting and applying appropriate accounting policies on the basis of the accounting rules adopted by the Commission's accounting officer[9]; making accounting estimates that are reasonable in the circumstances. The Director approves the annual accounts of the Agency after its accounting officer has prepared them on the basis of all available

---

[6] These include the balance sheet and the economic outturn account, the cash flow table, the statement of changes in net assets and a summary of the significant accounting policies and other explanatory notes.

[7] These comprise the budgetary outturn account and the annex to the budgetary outturn account.

[8] OJ L 357, 31.12.2002, p. 72.

[9] The accounting rules adopted by the Commission's accounting officer are derived from the International Public Sector Accounting Standards (IPSAS) issued by the International Federation of Accountants or, where relevant, the International Accounting Standards (IAS)/International Financial Reporting Standards (IFRS) issued by the International Accounting Standards Board.

information and established a note to accompany the accounts in which he declares, *inter alia*, that he has reasonable assurance that they present a true and fair view of the financial position of the Agency in all material respects.

(b) The management's responsibilities in respect of the legality and regularity of the underlying transactions and compliance with the principle of sound financial management consist of designing, implementing and maintaining an effective and efficient internal control system comprising adequate supervision and appropriate measures to prevent irregularities and fraud and, if necessary, legal proceedings to recover funds wrongly paid or used.

The auditor's responsibility

5. The Court's responsibility is, on the basis of its audit, to provide the European Parliament and the Council[10] with a statement of assurance as to the reliability of the annual accounts and the legality and regularity of the underlying transactions. The Court conducts its audit in accordance with the IFAC International Standards on Auditing and Codes of Ethics and the INTOSAI International Standards of Supreme Audit Institutions. These standards require the Court to plan and perform the audit to obtain reasonable assurance as to whether the annual accounts of the Agency are free from material misstatement and the transactions underlying them are legal and regular.

6. The audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the accounts and the legality and regularity of the underlying transactions. The procedures selected depend on the auditor's judgement, which is based on an assessment of the risks of material misstatement of the accounts and material non-compliance by the underlying

[10] Article 185(2) of Council Regulation (EC, Euratom) No 1605/2002 (OJ L 248, 16.9.2002, p. 1).

transactions with the requirements in the legal framework of the European Union, whether due to fraud or error. In assessing these risks, the auditor considers any internal controls relevant to the preparation and fair presentation of the accounts, as well as the supervisory and control systems that are implemented to ensure the legality and regularity of underlying transactions, and designs audit procedures that are appropriate in the circumstances. The audit also entails evaluating the appropriateness of accounting policies, the reasonableness of accounting estimates and the overall presentation of the accounts.

7. The Court considers that the audit evidence obtained is sufficient and appropriate to provide a basis for its statement of assurance.

Opinion on the reliability of the accounts

8. In the Court's opinion, the Agency's annual accounts present fairly, in all material respects, its financial position as at 31 December 2012 and the results of its operations and its cash flows for the year then ended, in accordance with the provisions of its Financial Regulation and the accounting rules adopted by the Commission's accounting officer.

Opinion on the legality and regularity of the transactions underlying the accounts

9. In the Court's opinion, the transactions underlying the annual accounts for the year ended 31 December 2012 are legal and regular in all material respects.

10. The comment which follows does not call the Court's opinions into question.

COMMENT ON INTERNAL CONTROLS

11. Whereas the Financial Regulation and the corresponding Implementing Rules provide for a physical inventory of fixed assets at least every three years, the Agency has not carried out a comprehensive physical inventory since 2009.

FOLLOW-UP OF PREVIOUS YEAR'S COMMENTS

12. An overview of the corrective actions taken in response to the Court's previous year's comments is provided in ***Annex I***.

This Report was adopted by Chamber IV, headed by Dr Louis GALEA, Member of the Court of Auditors, in Luxembourg at its meeting of 15 July 2013.

For the Court of Auditors

Vítor Manuel da SILVA CALDEIRA
President

ANNEX I

Follow-up of previous year's comments

Year	Court´s comment	Status of corrective action (Completed / Ongoing / Outstanding / N/A)
2011	The high level of carry-over is at odds with the budgetary principle of annuality.	**Completed**
2011	The Court identified the need to improve the documentation of fixed assets. Purchases of fixed assets are recorded at invoice and not at item level. When several new assets are covered by one single invoice, there is only one entry for all the purchased assets and the total amount.	**Ongoing**
2011	The Agency needs to improve the transparency of recruitment procedures. No adequate measures were taken to address the lack of transparency reported by the Court in 2010. The thresholds candidates had to meet in order to be invited to interview, the questions for written tests and interviews and their weightings were not prepared before the examination of the applications. Threshold scores for being put on a list of suitable candidates were not established before the examination of applications.	**Completed**

ANNEX II

European Network and Information Security Agency (Heraklion)

Competences and activities

Areas of Union competence deriving from the Treaty *(Article 114 of the Treaty on the functioning of the European Union)*	The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market. The Internal Market responsibility is a shared competence between the Union and the Member States (Article 4(2)(a) TFEU).
Competences of the Agency (*Regulation (EC) No 460/2004 of the European Parliament and of the Council)*	**Objectives** 1. The Agency shall enhance the capability of the Union, the Member States and the business community to prevent, address and respond to network and information security problems. 2. The Agency shall provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies. 3. The Agency shall develop a high level of expertise and use this expertise to stimulate broad cooperation between actors from the public and private sectors. 4. The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security. **Tasks** (a) To collect information on current and emerging risks that could produce an impact on electronic communications networks; (b) to provide the European Parliament, the Commission and European bodies or competent national bodies with advice and assistance; (c) to enhance cooperation between actors in its field; (d) to facilitate cooperation on common methodologies to address network and information security issues; (e) to contribute to awareness-raising on network and information security issues for all users by, *inter alia*, promoting exchanges of current best practices, including methods of alerting users and seeking synergy in public and private sector initiatives; (f) to assist the Commission and the Member States in their dialogue with industry; (g) to track the development of standards for products and services on network and information security; (h) to advise the Commission on research in the area of network and information security and the use of risk prevention technologies; (i) to promote risk assessment activities on prevention management solutions; (j) to contribute to cooperation with third countries and international organisations; (k) to express independently its own conclusions, orientations and to give advice on matters within its scope and objectives.
Governance	**Management Board** One representative from each Member State, three representatives appointed by the Commission, as well as three representatives, proposed by the Commission and appointed by the Council, without the right to vote, each of whom represents one of the following groups: (a) information and communication technologies industry; (b) consumer groups; (c) academic experts in network and information security.

	Permanent Stakeholders Group – 30 high-level experts representing the relevant stakeholders, such as the information and communication technologies (ICT) industry, ICT user organisations and academic experts in network and information security. – Following an open call, the Members are selected by the Executive Director, who after informing the Management Board of his decision, appoints the selected applicants *ad personam* for a term of office of 2,5 years. **Executive Director** Appointed by the Management Board, from a list of candidates proposed by the European Commission and following a hearing in the European Parliament, for a term of five years. **External audit** European Court of Auditors. **Internal audit** European Commission's Internal Audit Service (IAS). **Discharge authority** European Parliament on a recommendation from the Council.
Resources made available to the Agency in 2012 ***(2011)***	**Final Budget** 8,2 *(8,1)* million euro of which the Union subsidy is 100 % *(100 %)* **Staff at 31 December 2012** 44 *(44)* posts in the establishment plan, of which occupied: 42 *(41)*. Other posts occupied: 12 *(13)* contract staff, 4 *(4)* Seconded National Experts. Total staff: 58 *(58)*, undertaking the following tasks: – operational: 40 *(40)* – administrative: 18 *(18)*
Products and services in 2012 ***(2011)***	**WS[1]1: Identifying and Responding to the Evolving Threat Environment** The assessment of emerging threats is a necessary part of preparing for future challenges. The objective of this work stream was to derive a number of "IT-Security readiness statements" for various areas and government initiatives, in particular with regard to Member States and the Commission (e.g. by identifying emerging opportunities and risks of policy initiatives). This was achieved by assessing emerging opportunities and risks for areas and initiatives pertinent to various stakeholder communities. In particular, the Agency released a global report on the security threat landscape in Europe and more specific reports in the area of 'Consumerisation of IT', 'Cloud Computing' and 'Secure Procurement'. By analysing both opportunities and risks, ENISA was able to draw conclusions that reflect the trade-offs that institutions and businesses will need to make in real-time operational environments. This approach helps policy makers and business communities to take full advantage of innovative technologies and business models, whilst still maintaining a high degree of security. The approach made maximum use of existing cooperation agreements and support-relevant stakeholders in order to attain the objectives of the work stream. Number of deliverables: seven. **WS2: Improving Pan-European CIIP[2] and Resilience** The work carried out in this work stream was closely aligned with the CIIP Action Plan described in the Commission's communications of March 2009 and of March 2011 and were a natural continuation of work carried out as part of the work programmes of 2010 and 2011. Activities directly supported objectives laid down in the Internal Security Strategy document as well as the Digital Agenda. The core objective of work stream 2 was to assist Member States in implementing secure and resilient ICT systems and to increase the level of protection of critical information infrastructures and services in Europe. This involved a number of activities: – assisting relevant stakeholders to increase their level of efficiency and effectiveness; – supporting and promoting exercises on a pan-European level; – identifying and addressing the information security challenges in critical information infrastructures;

	– supporting and promoting the European Public Private Partnership for Resilience (EP3R); – identifying and addressing information security issues in Industrial Control Systems and Interconnected Networks; – supporting the EU-U.S. Working Group on Cyber-security and Cyber-crime established in the context of the EU-U.S. summit of 20 November 2010. Of these activities, the pan-European cyber security exercise is of particular note. The second such exercise was carried out on 4 October 2012, in which 339 organisations from across the EU participated. Number of deliverables: 13. **WS3: Supporting the CERT and other Operational Communities** The work packages described in this section are also closely aligned with the CIIP Action Plan described in the Commission's communication of March 2009, although the activities in this work stream are closely linked to the assistance and development of the CERT community. In the area of CERTs, ENISA aims to support the EU Member States to ensure that their respective national / governmental CERTs act as key components of their national capability for preparedness, information sharing, sustainable coordination and response. This is done by defining, together with the relevant stakeholders, baseline capabilities for national / governmental CERTs, and by providing necessary means to achieve that baseline. More specifically, the objectives of this work stream are: – to enhance the operational capabilities of Member States by helping the CERT community to increase its level of efficiency and effectiveness; – to support and enhance (co)operation between CERTs, and with other communities. As part of this work stream, ENISA examined legal and procedural obstacles faced by CERTs from Europe when cooperating and sharing information with CERTs and law enforcement from Third Countries and made recommendations on how to improve cooperation. Number of deliverables: 10. **WS4: Securing the Digital Economy** In this work stream, ENISA aims to identify measures that will enable the EU to manage properly the introduction and deployment of new interoperable services, while respecting the fundamental rights of individuals and using secure and trustworthy solutions. The work carried out in this area assisted public and private sector organisations in improving their security approach whilst developing sound procedures for managing personal data in line with the new proposed legislation on Data Protection. Support for the European Month of Network & Information Security for All was also carried out in this work stream. Number of deliverables: eight.

1. WS: Work stream.

2. CIIP: Critical Information Infrastructure Protection.

Source: Information supplied by the Agency.