Council of the European Union

Brussels, 5 December 2014
(OR. en)

16462/14

FIN 934

COVER NOTE

From:	Mr Vítor CALDEIRA, President of the European Court of Auditors
date of receipt:	23 October 2014
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 2013 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 2013.

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 2013 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 Union Agency for Network and Information Security for the financial year 2013

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 Union Agency for Network and Information Security(hereinafter “the Agency”, aka “ENISA”), which is located in Athens and Heraklion[2], was created by Regulation (EC) No 460/2004 of the European Parliament and of the Council[3] which, following different amendments was superseded by Regulation (EU) No 526/2013[4].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:

---

[2] The Agency’s operational staff were relocated to Athens in March 2013. Its administrative staff remain in Heraklion.

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

[4] OJ L 165, 18.6.2013, p. 41.

[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 2013, and

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

The management's responsibility

4. 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[8]:

(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 Executive Director approves the annual accounts of the Agency after its accounting officer has prepared them on the basis of all available information and established a note to accompany the accounts

---

[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] Articles 39 and 50 of Commission Delegated Regulation (EU) No 1271/2013 (OJ L 328, 7.12.2013, p. 42).

[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.

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 transactions with the requirements in the legal framework of the European Union, whether due to fraud or error. In assessing these risks, the auditor

[10] Article 107 of Regulation (EU) No 1271/2013.

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 2013 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 2013 are legal and regular in all material respects.

10. The comments which follow do not call the Court's opinions into question.

COMMENTS ON BUDGETARY MANAGEMENT

11. The overall level of committed appropriations was 94 %, which is explained mainly by the fact that additional funds requested from the Commission to finance the refurbishment of the new office in Athens were only approved in November 2013. In this context, an amount of 0,5 million euro that was not yet

committed at year-end was carried over following a Management Board decision.

12. In total, non-committed and committed appropriations carried over to 2014 amounted to 1,2 million euro (or 13,5 % of total appropriations). This mainly concerned title II (administrative expenditure) with 0,8 million euro or 59 % of title II appropriations. This high level is explained by the 0,5 million euro carry-over referred to in paragraph 11 and an additional 0,3 million euro carried over in order to finance furniture and networking equipment for the Athens office which was ordered towards the year-end.

OTHER COMMENTS

13. Operational staff of ENISA were relocated to Athens in 2013 while administrative staff remain in Heraklion. It is likely that the administrative costs could be reduced if all staff were centralised in one location.

14. According to the lease agreement between the Greek authorities, the Agency and the landlord, rent for the offices in Athens is paid by the Greek authorities. This rent is constantly paid with a delay of several months which is a business continuity and financial risk to the Agency: its operations would be affected, and its investments in office fitting and refurbishment would be lost, if the landlord were to cancel the lease agreement because of these delays in payment.

FOLLOW-UP OF PREVIOUS YEARS' COMMENTS

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

This Report was adopted by Chamber IV, headed by Mr Pietro RUSSO, Member of the Court of Auditors, in Luxembourg at its meeting of 16 September 2014.

For the Court of Auditors

Vítor Manuel da SILVA CALDEIRA
President

ANNEX I

Follow-up of previous years' comments

Year	Court's comment	Status of corrective action (Completed / Ongoing / Outstanding / N/A)
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.	**Completed**
2012	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.	**Ongoing**

ANNEX II

European Union Agency for Network and Information Security (Athens and 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." (*Article 114 TFEU*) Responsibility for the internal market is shared between the Union and the Member States (*Article 4(2)(a) TFEU*).
Competences of the Agency (*Quoted from Regulation (EU) No 526/2013 of the European Parliament and of the Council)*	**Objectives** 1. The Agency shall develop and maintain a high level of expertise. 2. The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security. 3. The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market. 4. The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents. 5. The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors. **Tasks** 1. The Agency shall perform the following tasks: (a) support the development of Union policy and law, by: (i) assisting and advising on all matters relating to Union network and information security policy and law; (ii) providing preparatory work, advice and analyses relating to the development and update of Union network and information security policy and law; (iii) analysing publicly available network and information security strategies and promoting their publication; (b) support capability building by: (i) supporting Member States, at their request, in their efforts to develop and improve the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, and providing them with the necessary knowledge; (ii) promoting and facilitating voluntary cooperation among the Member States and between the Union institutions, bodies, offices and agencies and the Member States in their efforts to prevent, detect and respond to network and information security problems and incidents where these have an

	impact across borders; (iii) assisting the Union institutions, bodies, offices and agencies in their efforts to develop the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, in particular by supporting the operation of a Computer Emergency Response Team (CERT) for them; (iv) supporting the raising of the level of capabilities of national/governmental and Union CERTs, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices; (v) supporting the organisation and running of Union network and information security exercises, and, at their request, advising Member States on national exercises; (vi) assisting the Union institutions, bodies, offices and agencies and the Member States in their efforts to collect, analyse and, in line with Member States' security requirements, disseminate relevant network and information security data; and on the basis of information provided by the Union institutions, bodies, offices and agencies and the Member States in accordance with provisions of Union law and national provisions in compliance with Union law, maintaining the awareness, on the part of the Union institutions, bodies, offices and agencies as well as the Member States of the latest state of network and information security in the Union for their benefit; (vii) supporting the development of a Union early warning mechanism that is complementary to Member States' mechanisms; (viii) offering network and information security training for relevant public bodies, where appropriate in cooperation with stakeholders; (c) support voluntary cooperation among competent public bodies, and between stakeholders, including universities and research centres in the Union, and support awareness raising, inter alia, by: (i) promoting cooperation between national and governmental CERTs or Computer Security Incident Response Teams (CSIRTs), including the CERT for the Union institutions, bodies, offices and agencies; (ii) promoting the development and sharing of best practices with the aim of attaining an advanced level of network and information security; (iii) facilitating dialogue and efforts to develop and exchange best practices; (iv) promoting best practices in information sharing and awareness raising; (v) supporting the Union institutions, bodies, offices and agencies and, at their request, the Member States and their relevant bodies in organising awareness raising, including at the level of individual users, and other outreach activities to increase network and information security and its visibility by providing best practices and guidelines; (d) support research and development and standardisation, by: (i) facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services; (ii) advising the Union and the Member States on research needs in the area of network and information security with a view to enabling effective responses to current and emerging network and information security risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively; (e) cooperate with Union institutions, bodies, offices and agencies, including those dealing with cybercrime and the protection of privacy and personal data, with a view to addressing issues of common concern, including by:

	(i) exchanging know-how and best practices; (ii) providing advice on relevant network and information security aspects in order to develop synergies; (f) contribute to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on network and information security issues, including by: (i) being engaged, where appropriate, as an observer and in the organisation of international exercises, and analysing and reporting on the outcome of such exercises; (ii) facilitating exchange of best practices of relevant organisations; (iii) providing the Union institutions with expertise. 2. Union institutions, bodies, offices and agencies and Member State bodies may request advice from the Agency in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services. 3. The Agency shall carry out tasks conferred on it by legal acts of the Union. 4. The Agency shall express independently its own conclusions, guidance and advice on matters within the scope and objectives of this Regulation.
Governance	**Management Board** The Management Board is composed of one representative of each Member State, and two representatives appointed by the Commission. All representatives have voting rights. Each member of the Management Board has an alternate to represent the member in their absence. Members of the Management Board and their alternates are appointed in light of their knowledge of the Agency's tasks and objectives, taking into account the managerial, administrative and budgetary skills relevant to fulfil the tasks of a member of the Management Board. The term of office of members of the Management Board and of their alternates is four years. That term is renewable. **Permanent Stakeholders Group** The Management Board, acting on a proposal by the Executive Director, appoints a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in network and information security, and representatives of national regulatory authorities notified under Directive 2002/21/EC as well as of law enforcement and privacy protection authorities. The term of office of the Permanent Stakeholders' Group's members is two and a half years. The Permanent Stakeholders' Group advises the Agency in respect of the performance of its activities. In particular, it advises the Executive Director on drawing up a proposal for the Agency's work programme, and on ensuring communication with the relevant stakeholders on all issues related to the work programme. **Executive Director** The Executive Director is appointed by the Management Board, from a list of candidates proposed by the Commission, following an open and transparent selection procedure, for a term of five years which is renewable. **Executive Board** The Executive Board is made up of five members appointed from among the members of the Management Board. It must include the Chairperson of the Management Board, who may also chair the Executive Board, and one of the representatives of the Commission. **External audit** European Court of Auditors. **Internal audit**

	Internal Audit Service of the European Commission. **Discharge authority** European Parliament on a recommendation from the Council.
Resources made available to the Agency in 2013 *(2012)*	**Final Budget** 9,7 million euro *(8,2 million euro)* of which the Union subsidy is 93 % (*100 %*) **Staff at 31 December 2013** 47 (*44*) posts provided for in the establishment plan, of which occupied: 43 *(42)*. Other posts occupied: 13 *(12)* contract agents; 3 *(4)* seconded national experts. Total staff: 59 *(58)*, undertaking the following tasks: operational: 42 *(40)* administrative: 17 *(18)*
Products and services provided in 2013 *(2012)*	**WS[1]1 - Evolving risk environment & opportunities** The objective of this work stream was to identify the most important evolving threats that are relevant to critical infrastructure and trust services. This was done by monitoring publicly available sources that publish threat-related data and by making a regular assessment of this data. Based on the analysis done, ENISA has proposed good practices and guidelines for mitigating these risks. The work has been performed in a collaborative manner with involved stakeholders and has used existing information sources wherever possible. The following objectives and results are achieved: • collection and consolidation of information on the emerging threat landscape • unification of available information sources under a common context. • involvement of relevant stakeholders • formulation of key messages (good practices and guidelines) to Member States and other stakeholders on how to improve their policies and capabilities. Number of deliverables: 7 *(7)* **WS2 – Improving Pan-European CIIP[2] & Resilience** Protecting Critical Information Infrastructures (CIIP) is a key priority for Member States, the Commission and industry (operators, service providers, manufacturers). By facilitating cooperation and coordination among Member States, ENISA has continued in this work stream to support all of these stakeholders in developing sound and implementable preparedness, response and recovery strategies, policies and measures to meet the challenges of a continuously evolving threat environment. The objectives and consequently results of this work stream were to: • finalise the evaluation of Cyber Europe 2012 and initiate the organisation and management of the next Cyber Europe 2014 • support the European Commission in implementing the EU's Cybersecurity Strategy • support Member States and EU Commission on the development of a sound European Cyber Crisis Cooperation Framework, national contingency plans and national exercises • enhance the co-operation of public and private stakeholders in activities related to CIIP through the EP3R • further support the Commission in its efforts to guide NRAs in the implementation of both Article 13a of the revised Framework Directive for electronic communications and Article 4 of the ePrivacy Directive and consult with stakeholders on the development of an integrated approach • examine the feasibility of the extension of Article 13a of the revised Framework Directive

	for electronic communications to new areas • enhance the security of Smart Grids and ICS-SCADA • assist interested Member States in the development of their national Governmental Cloud Strategies Number of deliverables: 16 *(13)* **WS3 - Enabling communities to improve network and information security (NIS)** The aim of this work stream was to help the communities that are instrumental in improving NIS to enhance their capabilities and to facilitate their work through the improvement of the legal and regulatory scenarios that they must comply with. ENISA has continued to work with CERTs to improve baseline capabilities in Europe. The Agency has also complemented this approach by addressing other communities that are active in improving NIS of their systems and infrastructure such as network and information systems managers as well as providers of security services within individual organisations (e.g. Information Security Officers (ISO)). The objectives and results of this work stream were: • to keep up to date and enhance the operational capabilities of Member States institutions by helping the CERT community to increase its level of efficiency and effectiveness and support to law enforcement agencies, the fight against cyber-crime, the protection of children and minors, etc.; • to support and enhance co-operation between CERTs and other communities; • to develop and promote the use of training and exercise material; • to support the implementation of pan-European trust marks (seals) in line with the Commission's actions in this field; • to investigate data leakage and implement appropriate data access controls; and • to review the situation on the use of cryptographic techniques in Europe, following up ENISA's work in 2011 in this field. Number of deliverables: 15 *(10)*

[1] WS: Work stream

[2] CIIP: Critical Information Infrastructure Protection

Source: Annex supplied by the Agency.