December 2012

Management Board Newsletter

A year of progress...

Dear members of the ENISA Management Board, welcome to the new issue of our MB Newsletter. You will find inside a summarised overview of all our deliverables published during 2012 as well as brief information of some of the main topics ENISA is currently tackling. As you know the Agency's mandate discussion is now close to its completion and we are happy that we will be hosting the next Management Board meeting on 21st March at Agency's seat in Heraklion, Crete. As ever, in the 2013, we'll continue to publish quarterly newsletters. Through this, we're able to provide you important dates as well as events, seminars and other information. Meanwhile the ENISA staff wish all of you and your families a safe and very happy holiday season!

With best wishes,
Udo Helmbrecht,
Executive Director,
ENISA

THE LATEST NEWS FROM ENISA...

September 2012, the European Commission adopted a strategy for "Unleashing the Potential of Cloud Computing in Europe".

For the first time, **in October,** a European Cyber Security Month (ECSM) took place as a pilot project across Europe. In this first pilot project, the Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain and the United Kingdom participated in various activities and events to raise awareness of cyber security. In addition Latvia and Council of the European Union officially supported the ECSM.

ENISA launched its social media channels on **19th September** along with its new redesigned website.

Twitter is ENISA's most popular social media channel with almost 500 followers in the first month of its online presence. Facebook network size is at the moment still growing. The number of fans is constantly rising and friends of fans (which is our potential reach audience) are more than 42.000.

At the 22nd meeting of the ENISA Management Board on **9th October**, the Board took the decision to re-appoint Mr Michail Christidis as ENISA's Accounting Officer. The full decision can be found at: **http://tinyurl.com/Accounting-Officer**

On 17th October the European Parliament Committee on Foreign Affairs adopted the "Report on Cyber Security and Defence". This report recognised that "Cyber Europe 2010", the first pan-European exercise on critical information infrastructure protection, which was carried out with the involvement of various Member States and led by ENISA, proved to be a helpful action and an example of good practices. Full report available here: **http://tinyurl.com/EP-report**

On **31st October** Mrs Jutta Haug, an MEP for the Socialists and Democrats Group in the European Parliament and a Vice Chair of the European Parliament's Budget Committee, visited ENISA's seat in Heraklion, Greece to learn more about the Agency's work and future plans.

Topics discussed included the ENISA Work Programme for 2013, the new ENISA Regulation proposal and future resourcing. Mrs Haug also saw presentations on ENISA's budget evolution, financial performance and latest European Court of Auditors report.

The right to be forgotten is included in the proposed regulation on data protection published by the European Commission in January 2012. The different legal aspects of the right to be forgotten (i.e. right to erasure or right to oblivion) have been debated in different contexts. On **20th November** ENISA published a technical paper focusing on the technical means to enforce or support "the right to be forgotten" in information systems; as can be seen from this paper, there are technical limitations and there is a further need for clear definitions and legal clarifications.

continued on page 2

PO Box 1309 71001 Heraklion Greece Tel: +30 2810 391 280 Email: info@enisa.europa.eu **www.enisa.europa.eu**
Follow ENISA on Facebook Twitter LinkedIn YouTube and RSS feeds

Latest News
continued from front cover

On **22nd November** ENISA launched an in-depth study on 30 different 'digital traps' or honeypots that can be used by Computer Emergency Response Teams (CERT)s and National/Government CERTs to proactively detect cyber-attacks. The study reveals barriers to understanding basic honeypot concepts and presents recommendations on which honeypot to use.

European Commission supports research on Cyber security. By next summer the Commission intends to publish the first Call for proposals in Horizon 2020. If you want to contribute to the discussion please fill in the questionnaire and send it back to functional mailbox. Depending on the feedback received, the DG CONNECT will plan the next steps to define the orientations for cyber security, privacy and trust activities in the Societal Challenge "Secure Societies" of H2020. A report addressing the industrial perspective and the report looking at the societal dimension of the workshops are a guide to help further discussions.

On **27th November** ENISA's Work Programme for 2013 has been adopted and published. The programme is the result of a consultation process involving both the ENISA Permanent Stakeholder Group (PSG) and Management Board (MB). This process has enabled the Agency to increase its focus on areas that are both strongly aligned with the European policy agenda and also considered as core areas of competency for the Agency.

In **November** the Agency launched an updated and expanded, comprehensive set of CERTs exercises consisting of a Handbook for tutors, a Toolset for students, and supporting material for hands-on training. The study material is looking in detail at 23 different exercises tailored for CERTs, but also usable for a wider community. Additionally a Roadmap has been created to answer the question 'How could ENISA provide more proactive and efficient CERT training?

Cooperation is key for Europe's cyber security

– Conclusion of ENISA Brussels event held on 27th November 2012

A high-level event organised by ENISA recognised closer cyber cooperation and mutual support as key factors for boosting cyber security for Europe's citizens, governments and businesses. The meeting brought together key figures from the European Parliament, European Commission and the computer industry.

Participants included Ms **Amelia Andersdotter, MEP and Mr Anthony Whelan, representing the Commission as Head of Cabinet for Vice President and Commissioner for the Digital Agenda Mrs Neelie Kroes. They were joined by Mr Paul Timmers, Director at DG Connect. Industry representatives were Mr Paul Nicholas, Senior Director, at Microsoft, and Mr Tom Koehler, CEO at Cassidian Cybersecurity, Germany.**

ENISA is currently in the process of having its working remit renewed and revised, with a new Regulation being finalised by the European Parliament and Council of Ministers. The new Regulation will enable ENISA to better support Europe's cyber security needs.

European Commission Vice President Neelie Kroes said: "The key to strong cyber security is sharing responsibility. That is the 'name of the game' for this event and for ENISA, and it's a more important challenge than ever as the role of the internet in our economy and society continues to grow rapidly."

Anthony Whelan provided the European Commission perspective, looking at the EU's forthcoming Cyber Security Strategy, and also gave an update on the progress of the new ENISA Regulation.

At the conference, ENISA's recent successes in building cooperation between different cyber communities was recognised. Examples included:

- Close cooperation with Member States, the Commission and now private sector on cyber security exercises;
- Supporting the set-up of up new national Computer Emergency Response Teams (CERTs) in Cyprus, Ireland, Malta and Romania and providing support for CERTS;
- Conducting the first Europe-wide cyber security exercise with the private sector involved, Cyber Europe 2012;
- Facilitating the first Annual Privacy Forum held, with the close support of the Cyprus EU Presidency;
- ENISA's ground-breaking role in producing the first ever comprehensive reports on cyber security breaches in Europe (under Article 13a of the EU telecoms directive)

Other areas addressed included the need for common standards in cyber security, to better enable Europe's IT industry to compete more effectively globally. Currently, other markets, notably the United States, are ahead of Europe in having common recognised standards.

First WP2013 tenders just launched...

Application of good practice for CERTs - Service aspects

Deadline: 25th January 2013

This Tender is divided into three LOTS.

LOT 1 - **Secure communication solutions for National/ Governmental CERTs: Stocktaking and Requirements**

This LOT focuses on the communication solutions CERTs are using. The selected contractor will run a stock taking study on the existing communication solutions (CRM, Ticketing systems, Incident handling communication platform, etc.) and their usages among the CERTs community. The stocktaking information will then be analyzed by the contractor together with the ENISA expert and discussed by a workgroup of experts in order to define functional and technical recommendations to better the efficiency of the exchange of information between national/governmental CERTs and other CERTs within their country.

LOT 2 **– Good Practice guide on Alerts Warnings and Announcements**

This LOT focuses on one of the core services of CERTs. The prospective contractor needs to identify and define the processes behind 'Alerts, Warnings and Announcements', run stocktaking on types, solutions, channels, tools used by CERTs in collecting information and alerting their constituency along with identifying incident handling methodologies.

LOT 3 - **ENISA CERT exercise material extended with cybercrime scenarios**

This LOT focuses on providing cybercrime related training and exercises for CERTs. The contractor will extend ENISA CERT exercise material with cybercrime scenarios and create a training suite suitable for use in TRANSITS I CSIRT Training Legal Issues package. Extended exercise and training material will cover legal, organisational, and technical aspects of cybercrime meeting the exact needs of the CERT community.

Enabling the information society - Securing personal data in online environments

Deadline: 28th January 2013

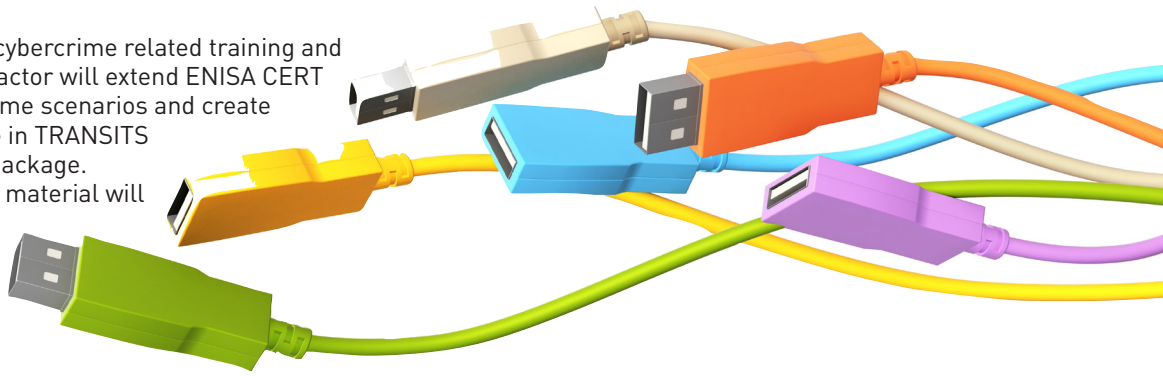
This Tender is divided into two LOTS.

LOT 1 – **Identifying security best practices for privacy protection purposes**

This lot is aiming to develop recommendations based on current security certification practice in the EU Member States. The selected contractor will take stock of security certification practice in the EU to provide recommendations for a future pan-European approach for privacy certification. At the same time, the contractor will identify existing implemented security measures to protect personal data in a couple of Member States.

LOT 2 – **Securing personal data in online environments**

The recommendations regarding encryption specifications and security solutions must be pro-actively reviewed in line with the changing circumstances (i.e. new vulnerabilities and attacks, better computational power). For this activity the contractor is expected to develop a methodology and structure for a new activity with the goal of establishing a list of recommended cryptographic algorithms (e.g. block ciphers, hash functions, signature schemes, etc) and recommended keysizes and other parameter settings (where applicable) to reach specified security objectives.



enisa jobs

ENISA Recruitment news

A new vacancy was published on 26/11/2012 to establish **a reserve list of Finance and Procurement Assistants**. Deadline to submit applications is 14/01/2013 at 14h00 Greek local time.

For more information please visit: http://www.enisa.europa.eu/recruitment/vacancies/finance-and-procurement-assistants-1

FORTHCOMING EVENTS...

Calendar of the ENISA organised events for January and February 2013[1]		
23rd – 25th January	In co-operation with ENISA 6th International Conference: Computers, Privacy and Data protection "Reloading Data Protection" http://www.cpdpconferences.org	Brussels, Belgium
5th – 6th February	Art 13a Working Group meeting	Riga, Latvia
12th February	Joint MB/PSG meeting	Athens, Greece

[1] For information purposes only. Dates are preliminary and might change unless the official invitations are distributed or published.

Calendar of the events ENISA has received invitations for January and February 2013		
22nd – 23rd January	NCSC Conference 2013 https://www.ncsc.nl/english/conference/conference-2013/programme/day-1.html	The Hague, Netherlands
28th – 31st January	FIRST/TF-CSIRT Technical Colloquium http://www.terena.org/activities/tf-csirt/meeting38/	Lisbon, Portugal
20th- 21st February	First Annual Conference on Cyber Defence "Cyber Strategy Formulation and Leadership"	Tartu, Estonia

Deliverables of Work Programme 2012 Work Streams

WORKSTREAM 1

Identifying and Responding to the Evolving Threat Environment

WORK PACKAGE 1.1 – Emerging Opportunities and Risks – Deliverables

D1 : Security threat landscape in Europe based on aggregated data collected from stakeholders **Under Review**
D2 : Consumerisation of IT (assessment plan) **Published**
D3 : Risks in Cloud Computing (assessment plan) **2012/12/14**

WORK PACKAGE 1.2 – Mitigation and Implementation Strategies – Deliverables

D1: Consumerisation of IT (implementation/mitigation plan) **Published**
D2: Risks in Cloud Computing (implementation/mitigation plan) **2012/12/14**

WORK PACKAGE 1.3 – Knowledge base – Deliverables

D1: Knowledge Base and associated procedures **Under Review**
D2: Stakeholder Requirements (Q4 - 2012) **Under Review**

WORKSTREAM 2

Improving Pan-European CIIP and Resilience

WORK PACKAGE 2.1 – Further Securing EU's Critical Information Infrastructures and Services – Deliverables

D1: Cyber Security Risks and Challenges of Smart Grids (carry over from 2011 **Published**
D2: Cloud Computing and Critical Services **2012/12/14**
D2: ENISA Report on Resilient Internet Interconnections (carry over from 2011) **Published**
D3: Good Practice Guide on Rerouting and Emergency Communications during Crisis **2012/12/14**
Extra mile: ENISA Appropriate security measures for SMART Grids **2012/12/14**
Extra mile: Legal Implications of Countering Botnets **Not to be published**

WORK PACKAGE 2.2 – Cyber Crisis Cooperation and Exercises – Deliverables

D1: Report of CYBER EUROPE 2012 **Restricted Access**
D2: Status Report on National and International CIIP Exercises **Published**
D3: Roadmap on Exercising for CIIP beyond 2012 **Restricted Access**
D4: ENISA Report on National Contingency Plans for CII (carry over from 2011) **Restricted Access**
Extra mile: EuroSOPEx 1 and 2 report **Restricted Access**
Extra mile: CESMO Report **Restricted Access**

WORK PACKAGE 2.3 – European Public Private Partnership for Resilience (EP3R) – Deliverables

D1: Dissemination Actions **Done**
D2: Management of EP3R Working Groups **Done**
D3: Good practice guide on cyber security strategies **2012/12/14**
D4: EP3R Activity Report and Position Papers **2012/12/14** **NOT an ENISA publication**
Extra mile: Incentives and Barriers of the Cyber Insurance Market in Europe **Published**
Extra mile: National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace **Published**
Extra mile: US-PPPs **Not to be published**
Extra mile: EP3R 2013 Work Objectives **2012/12/14** **NOT an ENISA publication**

WORK PACKAGE 2.4 – Implementing Article 13 a – Deliverables

D1: Three Article 13a workshops (Q1-Q4 2012) – Lisbon, Luxembourg, Mainz **Done**
D2: Framework for Collecting Annual National Reports of Security Breaches (Architecture and Implementation of Cyber incident reporting and analysis system – CIRAS) **Available upon request**
D3: Technical Guidelines on Incident Reporting v2.0 **2012/12/14**
Extra mile: Cyber Incident Reporting in the EU **Published**
Extra mile: 2012 Annual report about the 2011 incidents **Published**

WORKSTREAM 3

Supporting the CERT and other Operational Communities

WORK PACKAGE 3.1 – Support and enhance CERTs operational capabilities – Deliverables

D1 : An updated version of the "Baseline capabilities for national / governmental CERTs". **Approved, publication pending**
D2 : A status report on level of deployment of current set of baseline capabilities of national / governmental CERTs in the MS). **Approved, publication pending**
D3 : An updated and (where appropriate) extended set of CERT exercise material; a new scenario on "Early Warning". **Published**
D4 : A roadmap on how to enhance the roll-out of ENISA exercise material to the CERT communities. **Published**
D5 : Updated "ENISA Inventory of CERTs in Europe". **Published**
D6 : Complete update of Inventory document. **Published**

WORK PACKAGE 3.2 – Application of good practice – Deliverables

D1 : Support at least two TRANISTS basic courses, and in addition one TRANISTS enhanced (TRANSITS2) course. **Done**

WORK PACKAGE 3.3 – Support and enhance (co)operation between CERTs, and with other communities – Deliverables

D1 : Pilot of the EISAS activity in one Member State, with the help of ENISA and support by at least one other Member State (Q4 - 2012). **Approved, publication pending**
D2 : Updated good practice material for addressing NIS aspects of cybercrime. **Published**
D3 : Findings / conclusions from the 7th annual CERT workshop (report, to be shared only among workshop participants. **Available upon request**

WORKSTREAM 4

Securing the Digital Economy

WORK PACKAGE 4.1 – Economics of Security – Deliverables

D1 : Cost of Security Incidents **Under Review**

WORK PACKAGE 4.2 – Security governance – Deliverables

D1 : Survey on current practices in supply chain integrity. **Published**
D2 : Contributing in extending and implementing the provisions of Article 4 of ePrivacy Directive (Data Breach Notification). **Done**

WORK PACKAGE 4.3 – Supporting the development of secure, interoperable services – Deliverables

D2: (renamed) The right to be forgotten – between expectations and practice **Published**
D3 : Annual workshop on Privacy, Accountability and Trust in the Future Internet. **Organised on 10th-11th October**

Status as of 05.12.2012. highlighted in red

PO Box 1309 71001 Heraklion Greece Tel: +30 2810 391 280 Email: info@enisa.europa.eu **www.enisa.europa.eu**
Follow ENISA on Facebook Twitter LinkedIn YouTube and RSS feeds