Management Board Newsletter

December 2013

Work programme tenders launched 2014

Dear reader, welcome to our December Management Board newsletter.

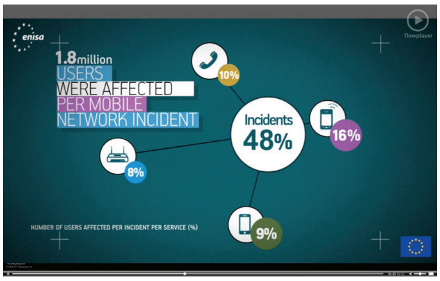
I am pleased to present the December issue of the MB Newsletter. This issue presents the latest ENISA activities in November and December, the list of ENISA deliverables to be published to implement Work Programme 2013 as well as tenders launched to start implementation of next year's Work Programme. As ever, in 2014 ENISA will continue to publish quarterly newsletters. This way we are able to provide you important dates as well as other relevant information. Meanwhile, the ENISA staff wish all of you and your families a safe and very happy holiday season!

With best wishes,

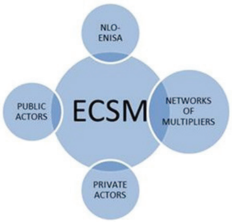
Udo Helmbrecht,
Executive Director, ENISA

The latest news from ENISA...

During the autumn 2013 several national authorities were visiting ENISA: Representatives from Croatian CERT teams; National Security Authority of the Czech Republic and Swedish Post and Telecom Authority (PTS).



To highlight the importance of incident reporting and to better explain the results of the 2012 incidents report, ENISA on **6th November** launched an animated, 2-minutes video. The video gives the answers to questions such as: "What kind of incidents were reported?", "What is the impact of these incidents on the electronic communication services?", "Which were the main causes of these incidents?", the video is available here: http://www.enisa.europa.eu/media/multimedia/art-13a-annual-incident-report-results-screencast


NLO-ENISA
PUBLIC ACTORS
ECSM
NETWORKS OF MULTIPLIERS
PRIVATE ACTORS

European Cyber Security Month (ECSM) organised throughout Europe in the month of October. It involved more than 60 stakeholders from 27 countries with ENISA national liaison officers (NLOs) playing a key role in reaching national communities. The dedicated website (http://cybersecuritymonth.eu/) provided a calendar of events for every country involved and a useful campaign toolbox.

The findings and documentation of the 2nd International Conference on Cyber Crisis Cooperation and Exercises have been summarised in a report published on **24th October**. The conference served as a key knowledge sharing platform both for national and governmental level cyber security experts. It also facilitated debate and information exchange, and offered networking opportunities for both technical experts as well as executive level stakeholders. The conference took place in Athens, 23-24th September.

ENISA's Head of Core Operations Department, Steve Purser participated in the IIEA Cybersecurity Conference that took place in Dublin on **15th November**. The key objective of the conference was to explore emerging cyber threats and opportunities for government and private sector collaboration in protecting the citizen online. He also gave an interview, available here: http://www.siliconrepublic.com/video/v/1350-iiea-cybersecurity/

ENISA was presented at the "Cloud for Europe" event (C4E) that was organised in Berlin, on **14th -15th November.** The Executive Director Prof. Udo Helmbrecht was speaking in the panel on "Enabling Trust in Cloud Computing", while Head of Secure Infrastructure & Services Unit, Evangelos Ouzounis presented ENISA's activities on Cloud Security in the panel "Cloud Computing in the digital service infrastructure". During 2013, ENISA has been supporting the work of the European Commission to implement the European Cloud strategy by participating in the Select Industry Group on cloud certification. The brief summary with ENISA's perspective on cloud certification can be found at: https://resilience.enisa.europa.eu/cloud-computing-certification

The first meeting of ENISA's electronic communications reference group, with experts from Telecom providers, took place on **21st November** at the Telecom Italia premises in Rome. The group's goal is to provide telecom providers with the opportunity to give feedback on ENISA's work and on telecom regulation in general.

On **22nd November** Russian delegation visited ENISA office in Athens. The Agency presented ENISA's work in the area of CIIP, CERT support, data protection and cyber security exercises. The visiting delegation informed ENISA about their activities in the field of the fight against cybercrime and CERT operation.

On **25th November** ENISA published new updates on the national cyber security strategies map. The Netherlands published their new, **updated NCSS**; Poland adopted the 2013 **NCSS**; and the **Spanish 2013 NCSS** was made available online; The Belgian cyber security strategy is under review to be published before the end of the year; Slovenia is preparing to adopt a new cyber security strategy by the end of 2013. You can find all strategies listed here: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

On **3rd December** the Competitiveness Council, following the positive vote in the European Parliament on 21 November, adopted the Regulation establishing Horizon 2020, the next EU research and innovation programme. Additional information on this programme can be found here: http://europa.eu/rapid/press-release_MEMO-13-1085_en.htm

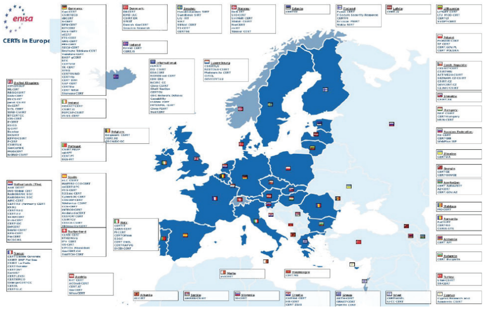
During Transport, Telecommunications and Energy Council (TTE) meeting on 5th December with Vice President of the European Commission Mrs Neelie Kroes participating, Member States held a policy debate on European Single Market for Electronic Communications and a Connected Continent. Ministers also discussed a progress report of the NIS Directive.

EU2013.LT

ChameleonsEye / Shutterstock.com

On **5th December** the ENISA Executive Director Prof Udo Helmbrecht took part in the public hearing of the European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee Inquiry on Electronic Mass Surveillance of EU Citizens.

The annual ENISA High Level Event took place in Brussels on **11th December** with more than 200 key policy actors, academia and industry partners attending. The focus of the debate was on cyber security and data protection; a discussion on soft law vs hard law and dialogue. The ENISA Executive Director Prof. Udo Helmbrecht mentioned the launch of the *ENISA annual Cyber Threats landscape report* in conjunction with the event. The Agency would most sincerely like to thank the State of Hessen for the excellent venue for the High Level Event, and for generously hosting this event in their new building, as well as the ESRT for excellent cooperation and support, as well as the speakers, and the audience, which all were necessary for making this even such a great success in terms of the quality of the debate, speakers, venue, topic, organisation, and attendance (more than 200 participants attending).



ENISA's new, updated and expanded Computer Emergency Response Teams (CERTs) Inventory was published on **13th December**, and now includes 222 CERTs. This is 13 teams more than the number reported at the previous update, in June 2013. The number shows the continuing expansion of CERTs teams across Europe, while at the same time reflecting ENISA's more detailed CERT mapping. The inventory and CERTs map are available online at the "CERT Inventory" and its subpages here: https://www.enisa.europa.eu/activities/cert/background/inv

ENISA's CERT map and inventory documents are updated twice a year. The next update is anticipated by June 2014.

SECURECLOUD2014

Call for papers for SecureCloud conference is open by **20th December** according to the guidelines published here: http://www.securecloud2014.org/Call_for_Presentations_SecureCloud_2014.pdf Cloud Security Alliance (CSA), ENISA and Fraunhofer-FOKUS have joined forces to organize the third edition of the SecureCloud conference, 1-2 April 2014, Amsterdam. SecureCloud 2014 focuses on legal issues, cryptography, incident reporting, critical information infrastructures and certification and compliance.

Calendar of events

ENISA has received invitations and plans to participate in Q1 2014

22-24 JANUARY
Brussels, Belgium
7th International Conference "CPDP: Reloading data protection"
http://www.cpdpconferences.org/

27-30 JANUARY
London, United Kingdom
Cyber Defence & Network Security Event

29-30 JANUARY
Brussels, Belgium
Conference "An Open and safe Europe – what next"

18-19 FEBRUARY
Cologne, Germany
StrategieTagen IT-Security

4-5 MARCH
Athens, Greece
18th Workshop on pan European Cyber Exercises

20-21 MAY
Athens, Greece
ENISA organised event Annual Privacy Forum 2014 (APF'2014)
http://privacyforum.eu/

ENISA is looking for new colleagues![1]

Seconded national experts with expertise in

Closing Date: Jun 30, 2014

- **Cyber Crisis Exercises and Cooperation,**
- **Critical Information Infrastructure Protection,**
- **Computer Emergency Response Teams (CERTs, aka CSIRTs)**

This call for SNE will remain open until 30 June 2014 at 14:00 (Greek local time). The first selection for secondment will take place no earlier than 2 months following the publication of this vacancy notice. Further evaluations will be carried out as necessary to fill possible on-going needs according to the number of applications received.

More information: *http://www.enisa.europa.eu/recruitment/vacancies/seconded-national-experts-6*

Experts in Network and Information Security

Closing Date: Jan 13, 2014

ENISA is looking for 4 experts in the field of Network and Information Security (NIS) in the areas of:

- **Secure Infrastructure and Services,**
- **Information Security & Data Protection,**
- **Operational Security.**

within the Core Operations Department (COD) of ENISA.

The experts in NIS must have the ability and willingness to contribute to more than one of the areas of the ENISA work programme as and when required. Allocation of tasks is based on an internal work plan developed by the Agency.

The experts in NIS must have the ability and willingness to contribute to more than one of the areas of the ENISA work programme as and when required. Allocation of tasks is based on an internal work plan developed by the Agency.

More information: *http://www.enisa.europa.eu/recruitment/vacancies/experts-in-nis*

[1] As published on 6th December 2013

ENISA launched tenders to start the implementation of

the Work Programme 2014

In 2013 Q3 the Agency launched two types of contracts: **Framework Contracts** for 3 years period and **Service Contracts** for 2014 only. Please see more information below.

Supporting the CERT community

Deadline: Jan 06, 2014

Framework Contracts with 'Re-opening of Competition' – maximum budget €1,000,000.00 over 3 years.

ENISA seeks to contract the services of a minimum of two (2) and maximum of four (4) service providers which can provide support for ENISAs CERT support programme. The successful bidders should be able to demonstrate significant experience and skills in this area, with emphasis on the aspects dealt with in the annual ENISA work programme in the area of CERT support. Additional consideration should be given, where applicable, to the various other aspects of ENISA activities.

Due to the diverse nature of the services requested, collaboration with other entities via subcontracting and/or consortium/groupings is encouraged.

Operational consultancy services in the field of cryptology

Deadline: Jan 07, 2014

Framework Contracts with 'Re-opening of Competition' – maximum budget €200,000.00 over 3 years.

ENISA seeks to contract service providers which can provide consultancy services in the field of cryptology, namely, cryptographic primitives, schemes, and protocols. Framework contracts (with re-opening of competition) will be awarded to a minimum of 2 and a maximum of 4 contractors. The successful bidders should be able to demonstrate significant experience and skills in this area, with emphasis on the aspects dealt with in the annual ENISA Work Programme in the area of Cryptology. Additional consideration should be given, where applicable, to the various other aspects of ENISA activities.

Supporting Cloud Security and Resilience activities

Deadline: Jan 13, 2014

Framework Contracts with 'Re-opening of Competition' – maximum budget €200,000.00 over 2 years.

By means of this Call for Tenders ENISA seeks to contract the services of a minimum of two (2) and maximum of four (4) service providers which can provide support in the field of security and resilience in cloud computing. The successful bidders should be able to demonstrate significant experience and skills in the area of cloud security and resilience, with emphasis on the aspects dealt with in the annual ENISA Work Programme.

Due to the diverse nature of the services requested, collaboration with other entities via subcontracting and/or consortium/groupings is encouraged.

Work Programme 2014 tenders continued...

Supporting Cyber Crisis Cooperation Exercises and other related Activities

Deadline: Jan 14, 2014

Framework Contracts with 'Re-opening of Competition' – maximum budget €400,000.00 over 3 years.

ENISA seeks to contract the services of a minimum of two (2) and maximum of four (4) service providers which can provide support for ENISA Cyber Crisis Cooperation and Exercises activities. The successful bidders should be able to demonstrate significant experience and skills in this area, with emphasis on the aspects dealt with in the annual ENISA Work Programme.

Due to the diverse nature of the services requested, collaboration with other entities via subcontracting and/or consortium/groupings is encouraged.

An evaluation framework for National Cyber Security Strategies

Deadline: Jan 24, 2014

Service Contract – maximum budget €40,000.00

In this study, ENISA would like to focus on the evaluation process of a NCSS, the process of checking the KPIs during the implementation phase and the steps towards the next NCSS for the Member States. The objective is to make a thorough good practice guide aimed at countries that have already drafted and implemented a NCSS and need now to start building on the next version.

Security measures for Inter-banking e-communications

Deadline: Jan 24, 2014

Service Contract – maximum budget €40,000.00

In a previous study on this subject, a number of conclusions were drawn, including the need for a better more precise understanding of the technical security measures usually adopted. This tender seeks to further examine the relevant issues such as; the actual Risk Awareness among ICT Professionals of the Finance sector, the State of prevention of Security risks, how are Incidents detected, how Incidents are mitigated and Security flaws fixed, etc.

Security and Resilience of electronic communications networks and services

Deadline: Jan 30, 2014

This Tender is divided into 2 LOTS. You may bid for just one or both LOTS – (Max budget – €100,000.00)

LOT 1 – Methodologies for the identification of Critical information infrastructure assets and services

ENISA requires a contractor which will assist the Agency to follow up the work of the 2013 "Guidelines for enhancing the resilience of data communication networks".

LOT 2 – Recommendations to address electronic communications dependencies on ICT products and services.

ENISA requires a contractor which will assist the Agency to determine: The existing dependencies in the electronic communications sector on ICT services and products supporting the core processes in providing public electronic communications networks and services; the most common types of ICT services and products being procured or outsourced; develop guidelines for providers, which allow them to better deal with security requirements in the procurement or outsourcing of ICT products and services. More information provided in the Tender Specifications.

Certification in Industrial Environments and Smart Grids

Deadline: Jan 31, 2014

This Tender is divided into 2 LOTS. You may bid for just one or both LOTS – (Max budget – €80,000.00)

LOT 1 – Certification of Cyber Security skills of ICS/SCADA Experts

Some of the objectives of this study are to:

- Assess the need among Member States (MS) and the relevant private sector for a voluntary or mandatory scheme for the Certification of Cyber Security Skills of ICS/SCADA experts;
- Identify the gaps between different certification schemes (if any) among MSs and the private sector and the challenges involved in developing Certification of Cyber Security Skills of ICS/SCADA expert's schemes. More information provided in the Tender Specifications.

LOT 2 – Smart Grid (Cyber) Security Certification

Some of the objectives of this study are to:

- Perform a desktop research on the existing security components' and systems' certification approaches for smart grids;
- Identify the gaps between different certification schemes (if any) among MSs and the challenges involved in further developing a harmonised certification approach. More information provided in the Tender Specifications.

A list of ENISA’s 2013 Work Programme publications

The following table contains links to the WP 2013 deliverables:

WS/WPK	Deliverable	Status
WS1	**Evolving Risk Environment & Opportunities**	
WPK 1.1	**Identification & mitigation of threats affecting Critical Information Infrastructure**	
D1	D1: A description of the most important risks identified by the assessment of the processed data, especially when they affect critical information infrastructures	Amending WP 2013 (Reduced scope) **ENISA Threat Landscape 2013** Publication expected on 11/12/2013 https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
D2	A Good Practice Guide on dealing with these risks, where appropriate together with proposals on how to coordinate these activities with other communities	Amending WP 2013 (Reduced scope) **Smart Grid Threat Landscape** Publication expected on 17/12/2013 https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/smart-grid-threat-landscape-and-good-practice-guide/
D3	Regular reports on identified risks and opportunities in the form of “Flash Notes” and other suitable formats	Flash Note: Can Recent Attacks Really Threaten Internet Availability? https://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability Flash note: Cyber-attacks – a new edge for old weapons https://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons
WPK 1.2	**Identification & mitigation of threats affecting Trust Infrastructure**	
D1	A description of the most important risks identified by the assessment of the processed data, especially when the affect trust infrastructure (technology and services)	Publication expected on 20/12/2013 1) **Trusted e-ID Infrastructures and services in EU -TSP services, standards and risk analysis report** https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-eid/ **Trusted e-ID Infrastructures and services in EU -TSP services, standards and risk analysis report** https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-eid/ 2) **Trusted e-ID Infrastructures and services in EU - Recommendations for Trusted Provision of e-Government services** https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/trusted-egov/
D2	A Good Practice Guide on dealing with these risks, where appropriate together with proposals on how to coordinate these activities with other communities	Publication expected on 20/12/2013 **eIDAS in e-finance and e-payment services** https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/eIDAS-in-e-finance-and-e-payment-services/
D3	Regular reports on identified risks and opportunities in the form of “Flash Notes” and other suitable formats	Flash notes merged with WPK 1.1. D3 Amending WP 2013
WS2	**Improving Pan-European CIIP & Resilience**	
WPK 2.1	**Cyber crisis cooperation**	
D1	Good Practice Guide on National Risk Assessment and Threat Modelling	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report
D2	International Workshop on Good Practices for Cyber	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conferences/2nd-enisa-conference/report
D3	Planning and Organising Cyber Exercises: Methodology, Templates and Toolkit	Amending WP2013 (cancelled)

WS/WPK	Deliverable	Status
WS2	Improving Pan-European CIIP & Resilience ontinued from page 6	
WPK 2.2	Facilitating Public-Private cooperation	
D1	Management of EP3R Constituency and Task Forces (workshops/calls)	**EP3R 2013 Activity Report** Publication expected on 18/12/2013
D2	Three Position Papers (one for each Task Force)	1) **EP3R – PP.TF.TermDef.CatAssets** Publication expected on 18/12/2013 www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tdca 2) **EP3R – PP.TF.IncidentMgmt.MutualAidStrategies** Publication expected on 20/12/2013 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-masim/ 3) **EP3R – PP.TF.TrustedInfSharing** Publication expected on 18/12/2013 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-tis/ 4) **MARIE Phase 2 Report** Publication expected on 1312/2013 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance/m-a-r-i-e-phase-ii-recommendations-report/
D3	Roadmap for ‘European Cyber-Security Month’ activities	Amending WP 2013 (Reduced scope) Publication expected on 16/12/2013 https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2013/ecsm-roadmap

WPK 2.3	Improving transparency of security incidents	
D1	Analysis of Annual 2012 Incident Reports and Recommendations for Mitigating Threats	Amending WP 2013 (Reduced scope) 1) **Annual Incident Report 2012** http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012 2) **National Roaming for resilience** https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience 3) **Power Supply Dependencies in the Ecomms Sector** Publication expected on 16/12/2013 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies
D2	Analysis of Incident Reporting Schemes for Cloud Computing	Publication expected on 13/12/2013 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing/
D3	Technical Implementation Guidelines for Data Breach Notification – Update	Publication expected 20/12/2013 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/proposal-for-one-security-framework-for-articles-4-and-13a

WPK 2.4	Enhancing the security of Governmental Clouds, Smart Grids and Interconnected Networks	
D1	Good Practice Guide for secure deployment of Governmental Clouds	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds
D2	Guidelines on testing the security of and patching ICS-SCADA systems	1) **Good practices for an EU ICS testing coordination capability** https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems 2) **White paper– Window of Exposure a real problem for SCADA systems** https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems
D3	Guidelines for enhancing the Resilience of Data Communication Networks	Amending WP 2013 (Reduced scope) Publication expected on 13/12/2013 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/guidelines-for-enhancing-the-resilience-of-ecommunication-networks

WS/WPK	Deliverable	Status
WS3	**Enabling Communities to Improve NIS**	
WPK 3.1	**Application of good practice for CERTs**	
D1	Secure communication's platform for European n/g CERTs (Requirements & stocktaking)	Detect, SHARE, Protect – Solutions for Improving Threat Data Exchange among CERTs https://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs
D2	EISAS – deployment in Europe (a feasibility study)	https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-deployment-feasibility-study
D3	Good practice guide on Alerts, Warnings and Announcements (including an inventory of Incident Response Methodologies)	"Best practice guide on Alerts, Warnings & Announcements". https://www.enisa.europa.eu/activities/cert/support/awa
D4	CERT Inventory; an extended overview (inventory and interactive map)	https://www.enisa.europa.eu/activities/cert/background/inv
WPK 3.2	**Enabling collaborative communities**	
D1	Good practice guide on the practical implementation of the "directive on attacks against information systems"	"A Good Practice Collection for CERTs on the Directive on attacks against information systems" https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems
D2	8th Annual CERT workshop report (public version)	"8th ENISA Workshop 'CERTs in Europe' report" https://www.enisa.europa.eu/activities/cert/support/files/8th-enisa-workshop-certs-in-europe-report
D3	CERT exercise material – extended – cybercrime scenarios (handbook and toolset)	"ENISA CERT exercise material extended with cybercrime scenarios" http://www.enisa.europa.eu/activities/cert/support/exercise
D4	New version of Baseline capabilities framework – international harmonisation (Status report on capabilities harmonisation with worldwide stakeholders) and appropriate ICS-CERT capabilities	1) Good practice guide for CERTs in the area of Industrial Control Systems https://www.enisa.europa.eu/media/press-releases/mitigating-attacks-on-industrial-control-systems-the-new-guide-from-enisa 2) CERT communities – Recognition mechanisms and schemes https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/
D5	CERT training support (TRANSITS and ENISA training portfolio activities)	No deliverable
D6	Good practice guide on harmonisation and implementation of legal frameworks for information sharing and international incident handling process	Amending WP 2013 (cancelled)
WPK 3.3	**Enabling the information society**	
D1	Supporting EC activities in the implementation of trustmarks. Identifying best practice from security certification that could be deployed for privacy certification and trustmark	1) **Paper on certification:** https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study 2) **Paper on trustmarks:** Publication expected on 19/12/2013 https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/on-the-security-privacy-and-usability-of-online-seals/
D2	Recommendations for best practice on data security of personal data/the use of cryptographic techniques for eGov services in Europe	1) **Paper on security of personal data:** https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/recommended-cryptographic-measures-securing-personal-data 2) **Cryptographic techniques for eGov services:** https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
D3	Good practices for security of electronic identification systems	Amending WP 2013 (Reduced scope) http://www.enisa.europa.eu/activities/identity-and-trust/trust-services/reports
D4	eID workshop	Amending WP 2013 (Reduced scope) Workshop conducted on 24th September in Brussels
D5	Dissemination activity (e.g. panel session) focusing on the work in the area of privacy and trust	Amending WP 2013 (Reduced scope)
Additional papers (extra miles)		
	Brokerage model of NIS in Education	Publication expected by 11/02/2014 on Safer Internet Day https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/brokerage-model-for-network-and-information-security-in-education/
	Securing personal data in the context of data retention. Analysis and recommendations	https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/securing-personal-data-in-the-context-of-data-retention/
	Proposal of methodology of severity assessment of data breaches	https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity