WORK PROGRAMME 2013

27 NOVEMBER 2012

Contents

ACRONYMS

AD: Administration Department

ADA: Administration Department Activity

APCERT: Asia-Pacific CERT

APT: Advanced Persistent Threat

CA: Certification Authority

CEO: Chief Executive Officer

CEP: Cyber Exercises Platform

CERT: Computer Emergency Response Team

CII: Critical Information Infrastructures

CIIP: Critical Information Infrastructure Protection

CIP: Competitiveness and Innovation Programme

CISO: Chief Information Security Officer

COM: EU Commission

CSIRT: Computer Security Incidents Response Teams

D: Deliverable

DG: Directorate-General

DPA: Data Protection Authorities

EC: European Union Commission

ED: Executive Director

EDPS: European Data Protection Service

EGC: European Government CERTs

EFMS: European Forum for Member States

EFTA: European Free Trade Association

eID: electronic Identity

EISAS: European Information Sharing and Alert System

ENISA: European Network and Information Security Agency

EP3R: European Public Private Partnership for Resilience

ERNCIP: EU Reference Network for Critical Infrastructure Protection

EU: European Union

EuroSCSIE: European SCADA and Control Systems Information Exchange

FAP: Finance, Accounting & Procurement section

FIRST: Forum of Incident Response and Security Teams

FP (7): Framework Programme (7)

IaaS: Infrastructure as a Service

ICS: Industrial Control Systems

ICT: Information and Communication Technologies

IDABC: Interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens

IS: Information Systems

ISAC: Information Sharing & Analysis Centre

ISO: International Organization for Standardization

ISO: Information Security Officer

ISP: Internet Service Providers

ITFMU: Information Technology & Facilities Management Unit

ITU: International Telecommunication Union

IXP: Internet exchange point

LEA: Law Enforcement Agency

LHR: Legal & Human Resources section

MB: Management Board

MISS: Missions

MS: Member States

n/g CERT: National / Governmental CERT

NCO: National Contact Officer

NCP: National Contigency Plans

NIS: Network and Information Security

NISHA: Network for Information Sharing and Alerting

NLO: National Liaison Officer

NRA: National Regulatory Authority

PaaS: Platform as a Service

PAU: Public Affairs Unit

PKI: Public Key Infrastructure

PPP: Public Private Partnership

PSG: Permanent Stakeholders Group

Q: Quarter

R&D: Research and Development

RIM: Research In Motion

SaaS: Software as a Service

SCADA: Supervisory Control And Data Acquisition

SME: Small and Medium Enterprise

SOC: Security Operations Centres

SR: Stakeholder Relations

STORK: Secure *IdenTity* AcrOss BordeRs LinKed

TF-CSIRT: Task Force of Computer Security Incidents Response Teams

TISPAN: Telecommunications and Internet converged Services and Protocols for Advanced Networking

TCD: Technical Competence Department

US: United States of America

WP: Work programme

WPK: Work Package

WS: Work Stream

1 Executive Summary

1.1 Introduction

The work programme for 2013, as contained in this document, is a 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.

The content of the work programme is a logical extension of work carried out in previous years, but is increasingly focused on a common set of issues. In work stream 1 for example, which is concerned with understanding the evolving threat environment and defining suitable mitigation strategies, the areas of application are Critical Infrastructure and Trust Infrastructure. This focus on core issues will allow the Agency to exploit synergies between the different activities that constitute the work programme as a whole and is expected to provide stakeholders with a more holistic view of the state of NIS in these areas.

As in previous years, ENISA recognises the need to avoid duplication of work and has sought to define activities that are complementary to those undertaken by other European bodies or by other stakeholder communities in general.

1.2 Structure

1.2.1 Core operational activities

The core operational activities covered by the 2013 Work Programme have been structured as three separate work streams. These work streams are as follows:

- WS1: Evolving risk environment & opportunities
- WS2: Improving pan-European CIIP & resilience
- WS3: Enabling communities to improve NIS

These work streams essentially constitute an extension of the work carried out in the 2012 work programme, but introduce changes of priority and focus that were agreed during the strategic Management Board meeting of 29 November 2011. Input from the Permanent Stakeholder Group (PSG) was provided to the Management Board prior to this meeting.

The three work streams presented in this document cover the evolution of the global threat environment, the need to continue to improve Critical Information Infrastructure Protection (CIIP) across the EU and the need to continue to support the CERT and other operational communities.

In addition, supporting work will continue in the form of a set of horizontal activities. Press and Communications will also be planned as a separate activity within the Agency, as in previous years.

1.2.2 Operational Horizontal activities

This work programme regroups all the following activities into a single chapter, under the general heading of 'Horizontal Activities':

- Stakeholder Relations
- Project Support Activities
- Policy & Public Affairs

1.2.3 Administration activities, Directorate & Quality Control

1.2.4 Directorate, Quality Control & Administration activities,

The Directorate consists of the Executive Director and his personal assistant. The Executive Director is responsible for the overall management of the Agency.

The Administration Department (AD) consists of two main sections Finance, Accounting & Procurement (FAP) and Legal & Human Resources section (LHR).

The Quality Control Advisor reports directly to the Executive Director.

1.2.5 IT & Facilities Management activities

The IT and Facilities Management Unit (ITFMU) supports the smooth running of the Agency by offering IT, Physical Security and Facilities Management services.

In 2011 the Agency started to implement procedures for handling classified information. This project will be continued in 2013.

Facilities Management is also responsible for the move to the new office building.

The Head of ITFMU reports directly to the Executive Director.

2 Policy Context and Strategic Outlook

The Agency situates its work in the wider context of a legal and policy environment as pointed out below. Its activities and tasks are fulfilled as defined by its Regulation and integrated in this larger policy context.

The ENISA-Regulation[1]

All activities and tasks fulfilled by the Agency are fulfilled on the basis of the founding ENISA-Regulation.

The Strategy for a Secure Information Society[2]

The purpose of this Communication was to revitalise the European Commission strategy set out in 2001 in the Communication "Network and Information Security: proposal for a European Policy approach". The strategy reviewed the state of threats to the security of the Information Society and proposed additional steps to be taken to improve network and information security (NIS).

The Council Resolution of December 2009[3]

The Council Resolution on a collaborative European approach on Network and Information Security of 18 December 2009 builds on a number of EU strategies and instruments developed in recent years. It provides political direction on how the Member States, the Commission, ENISA and stakeholders can play their part in enhancing the level of network security in Europe.

The Council conclusion on CIIP of May 2011[4]

The Council Conclusion take stock of the results achieved since the adoption of the CIIP action plan in 2009, launched to strengthen the security and resilience of vital Information and Communication Technology Infrastructures.

The Commission proposal on the future of ENISA[5]

This document spells out a proposal from the European Commission for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA). The proposal complements regulatory and non-regulatory policy initiatives on Network and Information Security taken at Union level to enhance the security and resilience of ICTs. The proposal mentions several of the on-going developments in NIS policy (notably those announced in the Digital Agenda for Europe) that would benefit from the support and expertise of ENISA.

The Electronic Communications Regulatory Framework[6]

The review of the EU electronic communications regulatory framework and, in particular, the new provisions of articles 13a and 13b of the Framework Directive and the amended article 4 of the e-Privacy Directive aim at strengthening obligations for operators to ensure security and integrity of

---

[1] March 2004 establishing the European Network and Information Security Agency.

[2] European Commission on a Strategy for a Secure Information Society, COM(2006)251

[3] Council resolution of 18 December, 2009 'On a collaborative approach to network and information security (2009/C 321 01)

[4] Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)

[5] The European Commission *Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)* (14358/10)

[6] Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

their networks and services, and to notify breaches of security, integrity and personal data to competent national authorities and assign to ENISA specific tasks.

The CIIP Action Plan[7]

The Commission Communication "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" calls upon ENISA to support the Commission and Member States in implementing the CIIP Action Plan to strengthen the security and resilience of CIIs.

The Commission Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011[8]

In this communication, the Communication takes stock of the results achieved since the adoption of the CIIP action plan in 2009 launched to strengthen the security and resilience of vital Information and Communication Technology infrastructures. The next steps the Commission proposes for each action at both European and international level are also described.

Review of the Data Protection Legal Framework

On 25/01/2012, the European Commission published its proposal for a regulation on data protection[9]. This regulation will replace the existing Data Protection Directive. It encompasses many of the concepts described above, promoting privacy by design and data protection by default while including provisions for remedies, liability and administrative sanctions in case of non-compliance. ENISA will support the implementation of the new regulation on data protection.

The Single Market Act[10]

In April 2011, the European Commission adopted a Communication, the Single Market Act, a series of measures to boost the European economy and create jobs. This includes notably the key action entitled 'Legislation ensuring the mutual recognition of electronic identification and authentication across the EU and review of the Directive on Electronic Signature's. The objective is to make secure, seamless electronic interaction possible between businesses, citizens and public authorities, thereby increasing the effectiveness of public services and procurement, service provision and electronic commerce (including the cross-border dimension).

The Digital Agenda[11]

The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy, and provides an action plan for making the best use of ICT to speed up economic recovery and lay the foundations of a sustainable digital future. The Digital Agenda for Europe outlines seven priority areas for action, in the context of which it also attributes a significant role to ENISA as well as to its stakeholders, especially in the context of pillar III (information security) it also attributes a significant role to ENISA as well as to its stakeholders.

---

[7] Commission Communication of March 2009, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149.

[8] "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011 and the Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)

[9] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed on 20.02.2012)

[10] Single Market Act – Twelve levers to boost growth and strengthen confidence "Working Together To Create New Growth", COM(2011)206 Final

[11] *A Digital Agenda for Europe*, COM(2010)245, May, 2010.

The Internal Security Strategy for the European Union[12]

The Internal Security Strategy lays out a European security model, which integrates among others action on law enforcement and judicial cooperation, border management and civil protection, with due respect for shared European values, such as fundamental rights. This document includes a number of suggested actions for ENISA.

The Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary

This conference took place on 14-15 April 2011 and was a natural extension of the "Tallinn process" initiated by the 2009 Ministerial CIIP Conference in Estonia under the Czech Presidency of the EU. On this occasion, Vice President of the European Commission, Neelie Kroes, Digital Agenda Commissioner, acknowledged the progresses made by Member States but also called upon for further actions and stressed the importance of international cooperation. In particular, as a follow-up to the Conference, VP Neelie Kroes called on ENISA to intensify its activity of promoting existing good practices by involving all Member States in a peer-learning and mutual support process with the aim to promote faster progress and bring all Member States on par. VP Neelie Kroes called on ENISA to establish a highly mobile dedicated team to support such process.

The work streams (WS) that are described in this document have been developed in this context and they support this overall political agenda.

European Strategy for Cyber Security[13]

At the time of writing, the European Strategy for Cyber Security is still under development. The text that follows is therefore a reflection of the current state of affairs and may well change.

The goal of the initiative is to propose a comprehensive Cyber Security Strategy for Europe. It will be associated with one or more legal instruments, and it will aim to ensure a secure and trustworthy digital environment, which protects and promotes fundamental rights and core values:

- Improve security of network and information systems
- Prevent and fight cybercrime
- Ensure coordinated EU international policy

Strategic priorities and actions include the following:

- Fostering preparedness, response and cooperation
- Developing an integrated internal market for security solutions
- Prevention of and response to cybercrime
- Raising awareness, training and education
- Fostering R&D investments
- Ensuring a coherent international cyber policy and promoting EU core values
- Global capacity building on technology, reliable access and security
- Developing cyber defence capabilities.

[12] An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf

[13] http://www.europarl.europa.eu/document/activities/cont/201207/20120712ATT48826/20120712ATT48826EN.pdf

EC proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market

The aim of the European Directive 1999/93/EC[14] on a community framework for electronic signatures was the legal recognition of electronic signatures. Assessing the need for secure and seamless electronic transactions as well as the shortcomings of the Directive, the European Commission (EC) has adopted on 04/06/2012, a proposal[15] for a Regulation on electronic identification and trusted services for electronic transactions in the internal market.

Strategic Outlook

The emergence of cyber security, where the goals and objectives are linked to global considerations and the emphasis is on international collaboration, represents a fundamental change in the way in which information security is evolving. The core mission of ENISA – to foster the development of a strong culture of NIS throughout the EU is perfectly aligned with this development and the Agency is well positioned to assist the Member States and the Commission and in defining and implementing effective strategies for dealing with cyber threats throughout the next decade.

Over the last few years, the ENISA work programme has been dominated by three core areas of activity and a number of horizontal activities. Core activities have been in the areas of threat/risk assessment, Critical Information Infrastructure Protection (CIIP) and supporting operational communities (notably the CERT community). The main supporting activities have been in the area of risk assessment, standardisation and, more recently, privacy and data protection. The Agency has also put a considerable amount of effort into improving the way it interacts with its different stakeholder communities and ensuring that stakeholder requirements are well understood and reflected by the work programme.

Whilst the core areas have not changed, the approach to delivering services has changed significantly. The Agency has developed from an 'activities-based' approach, through a 'deliverables-based' approach to what could now be best described as an impact driven approach. This impact driven approach is characterised by three separate considerations. Firstly, the Agency has broadened its definition of deliverables to include activities as well as reports – examples of this include the pan-European cyber security exercise or assisting Member States in the creation of a national/governmental CERT. Secondly, ENISA works increasingly through its stakeholder communities, using their expertise to generate results that are valuable for the whole community. This is not only typified by the core activity of spreading good practice but is also reflected in a strong participation in ENISA projects by our stakeholder communities. Another example is provided by the way in which ENISA approaches the question of threat analysis and risk management – whereas in the past ENISA experts carried out such risk analyses themselves the current approach is to make optimal use of the numerous sources of risk and threat data that are being produced elsewhere and to tailor this data to the needs of specific stakeholder communities. This avoids duplication of work and offers better scalability. Finally, by introducing the Mobile Assistance Team (MAT) and making better use of the Article 10 regulation, ENISA provides the EU institutions and the Member States with mechanisms allowing them to call upon the services of the Agency for specific issues that are not covered by the work programme. This has resulted in a more agile approach to achieving our mission.

This development has been mirrored by a corresponding evolution in the way in which the annual work programme has been developed. Since 2009, ENISA has employed a structured method for developing the work programme based exclusively on the input of its stakeholder communities.

[14] http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett

[15] http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

Proposals for individual work packages are assessed by these communities using an agreed set of criteria that help ensure that the Agency achieves real impact.

Assuming that the process for agreeing the new mandate for ENISA completes successfully, the strategic outlook for ENISA is essentially a logical continuation of these developments. ENISA will continue to organise its work in terms of long-term strategic areas, based on risk/threat assessment, CIIP and community building in the short-term (1-3 years) and evolving to reflect the priorities of our stakeholders. It is worth noting however that each of these areas represents a broad category of issues and there is considerable scope for modifying the focus of the work in each area – in this sense the areas are well chosen, providing a broad area of focus but not being unnecessarily restrictive.

In the future, standardisation and other issues that are common to many different areas will be managed as horizontal activities, where all ENISA experts are expected to develop the necessary experience and skills to integrate these activities into their respective projects.

Where the operating model is concerned, we continue to look for improvements in the way in which we work with stakeholders to define the annual work programme and how this is linked to more strategic objectives.

3 Core operational activities

3.1 Introduction

The core activities of ENISA for 2013 have been grouped into three work streams (WS):

- WS1- Evolving risk environment & opportunities, will focus on informing policy makers and private sector companies on how risks are evolving and suitable mitigation strategies for handling these risks. The level of detail of the analysis will be sufficient to support strategic and policy decisions. In addition to informing policy makers, the objective is to mobilise stakeholder communities in achieving common goals and to align strategies and methods. The focus of this work stream will be on the areas of critical information infrastructure and trust infrastructure.
- WS2- Improving pan-European CIIP & Resilience, will address the security of electronic communications and information systems used in the operation of Critical infrastructures and thus the outcome of this WS will be addressed to the managers of the ICT systems using those infrastructures. The beneficiaries of the work achieved in this WS will be the providers of the services critical for the society.
- WS3 – Enabling communities to improve NIS, is the WS that will address the security of the underlying internet communications, not from the service providers' viewpoint, but from the viewpoint of the users of the internet services. The results of this WS will be addressed to the Network & Internet security managers, as well as other security mechanisms implementation and validation communities, but from the point of view of the "implementer". The beneficiaries of those activities will be the Information Security Officers of the organisations, i.e. the "internal" security service providers.

3.2 WS1- Evolving risk environment & opportunities

3.2.1 Overview

New technologies, infrastructures and services are becoming increasingly relevant in the day to day activities of citizens and businesses. The crash of RIM (Research In Motion, Blackberry)[16] in October 2011 and a bad configuration update in internet routers[17] that caused outage (delays) in the network worldwide, are examples of the dependency of many business and private activities on ICT infrastructures and services. Beyond causing impact on businesses and quality of life, such failures can seriously affect society as a whole when critical infrastructure is at stake.

In addition, it is clear that the role of trust infrastructures and services is fundamental to the correct functioning of the information society, as these services provide a framework within which business applications can function as intended. For this reason, trust infrastructure and services can be considered as a particularly important class of critical infrastructure components.

The objective of this work stream is to identify the most important evolving threats that are relevant to critical infrastructure and trust services, by monitoring publicly available sources that publish threat-related data and making a regular assessment of this data, with the goal to suggesting guidelines and support for the mitigation of these risks (based on current best practice). This approach should support the maintenance of a secure and resilient infrastructure for those services that are critical to Society (such as e-commerce, e-government, e-health, financial, but also others) and should also help to ensure that the associated trust services (such as e-Identity) are themselves both secure and resilient.

Justification

An important role of ENISA is to provide its stakeholders with guidelines on topics that are related to Network & Information Security (NIS) - especially those topics that are associated with the correct functioning of the Internet infrastructure and the services that use this infrastructure. In this work stream, ENISA will identify and analyse NIS issues of critical infrastructure and services crucial for society (in particular threats and risk exposure of important assets) as regards the impact that failure might have on various stakeholder groups including industry, public sector and (to a limited extent) end users. Particular focus will be put on informing policy makers and private sector on how risks are evolving and proposing suitable mitigation strategies.

It is also expected that the results of this work will contribute towards the identification of effective practices in Cyber Security: working on emerging threats with the involvement of stakeholders will help to develop an adequate understanding of the threat landscape. This in turn will facilitate the compilation of commonly accepted threat information and common paths of actions in order to help the Member States increase the level of preparedness within the EU.

The work will be performed in a collaborative manner with involved stakeholders and will use existing information sources wherever possible. Existing assessments will be complemented as appropriate. Such material will have a special focus on the needs of particular stakeholder groups associated with critical and trust infrastructures.

The following benefits are foreseen:

- The collection and consolidation of information on emerging threat landscape
- The unification of available information sources under a common context.

[16] http://www.guardian.co.uk/technology/2011/oct/10/blackberry-outage-affects-bbm-services

http://www.zdnet.com/blog/btl/blackberrys-outage-post-mortem-where-did-it-all-go-wrong/60801

[17] http://www.theregister.co.uk/2011/11/07/global_net_outage/

- The involvement of relevant stakeholders
- The formulation of key messages to the Member States on how to improve their policies and capabilities.
- The results will also be used as input for the work in WS2 that deals with the creation or the improvement of national cyber security strategies.

Specific Policy Context

Specific policy references for this work stream are as follows:

- ENISA Regulation
- Directive 2009/140/EC, Art. 13a
- The Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

Overall Objectives

The objectives of this Work Stream are:

- To support the development and maintenance of new security technologies and services, by ensuring that these reflect the evolving threat landscape. ENISA will seek to align its recommendations with other European programs and initiatives wherever possible (e.g. FP, CIP, EU Strategy for Cyber Security, etc.).
- To analyse and interpret information that is derived from public resources (analysis of primary sources), from a neutral stand-point and to complement and adapt this information to the needs of ENISA's stakeholders as required.
- To contribute to aligning the perspectives of governments and private sector and provide clear direction regarding issues of mid- and long-term importance to increase confidence in critical and trust infrastructures and reduce risk exposure. In addition to these more general objectives, the work in this WS will focus on the following sectors:
    - Critical information infrastructures and services, in particular those that could relate to current and future policy developments (e.g. EU Strategy for Cyber Security)
    - Trust services and infrastructures used to provide basic security properties to other services and applications, such as privacy, identity preservation and trust, personal data protection, etc. This covers the trustworthiness of the security services themselves, analysing its requirements and dependencies.

The results of this work stream will, among others, be addressed to policy makers, managers and operational staff (e.g. CEO, CISO, Operators of companies running critical infrastructures and/or trust services), providing them with guidelines to identify controls and, where appropriate, regulations needed to promote the use of the trust services to mitigate the risks critical services have.

The beneficiaries of the application of these guidelines could be the technology and services providers themselves, thanks to the improvement on the quality and efficiency of the security offered by their products to their customers and the trustworthiness generated on them to use those products.

3.2.2 Work Packages

The following work packages constitute the Work Stream:

- WPK 1.1: Identification and Mitigation of Threats Affecting Critical Infrastructure.
- WPK 1.2: Identification and Mitigation of Threats Affecting Trust Infrastructure.

3.2.3 WPK 1.1: Identification and Mitigation of Threats Affecting Critical Information Infrastructure

Desired Impact

- At least 10 different organisations are using the conclusions of these analyses by 2014. The produced material is recognised as a neutral source of information
- At least 5 policy makers in cyber security have used the produced information

Description of tasks

The objective of this work package is to identify risks and corresponding mitigation measures related to the use of critical infrastructures, services and applications. Critical infrastructures to be considered in this workpackage[18] are (among others) from the following areas: commerce (e.g. payment systems), government (e.g. governmental service portals), health (e.g. e-Health applications), financial services (e.g. key ICT components of payment infrastructures). In the risk analyses to be performed, additional issues will be taken into account where appropriate, such as:

- Impact on data protection/privacy
- Economic aspects
- Opportunities
- Enhancement of trust and
- Dissemination of results

The overall focus shall be the identification of the threat landscape including political, social, economic and technical threats. At the same time ENISA will describe requirements for risk mitigation tailored to affected stakeholders. As mentioned, the approach followed will be to amend/complement existing analyses and put them in the context of the target stakeholder groups. For the completion of existing analysis, existing methods will be used. The method used will be appropriately referenced/documented so that it can be reused by interested parties. The developed material could additionally serve as a basis for knowledge transfer between several target groups (e.g. governments, industry, end users, etc.). As such it will help different stakeholder groups to:

- learn from each other, i.e. through brokerage of good practices,
- align approaches where this makes sense and
- mobilise to reduce risks and be better prepared to deal with these risks

Results will be aligned with the Cyber Security Strategy of the European Commission and other cyber security activities of European Bodies.

Outcomes & deadlines

The outcome of this WPK will be:

- D1: A description of the most important risks identified by the assessment of the processed data, especially when they affect critical information infrastructures
- D2: A Good Practice Guide on dealing with these risks, where appropriate together with proposals on how to coordinate these activities with other communities.
- D3: Regular reports on identified risks and opportunities in the form of “Flash Notes” and other suitable formats

[18] As decided in the joint MB/PSG meeting in February 2012

Stakeholder impact

This WPK is mostly addressed to managers and maintainers of Information Systems (IS), applications service providers, and the providers of the infrastructures needed for those services being widely accessible and interoperable. They will get the following benefits:

- Description of risks and threats, together with mitigation measures and strategies
- Consolidation of existing information
- Guidelines on mitigation of (emerging) threats on
- Use of existing findings in own activities to improve existing controls
-

As result of the improvement of the security of society's critical infrastructures and services, the following stakeholders will benefit from this work:

- Policy Makers (Member States and EU Institutions)are expected to use the results to support on-going activities (e.g. policy actions, stakeholder dialogue, interaction with MS) and should also profit from useful overviews of emerging threats to critical infrastructures and services and related information to increase mitigation capabilities
- Members of industry (for example companies running parts of critical infrastructures and services) will be able to use the consolidated information to better secure their own activities and assets. In particular, industry should be able to Increase the effectiveness of mitigation through knowledge transfer and capacity building and reach new stakeholder segments (e.g. Policy Makers, SMEs)
- Supporting parties (standardisation institutes, research organisations) will be able to develop common standards based on good practices and to initiate research in relevant areas to contribute towards mitigation of emerging risks. They should also be able to increase effectiveness of mitigation through knowledge transfer and capacity building

Resources

- 15 person months
- 80 kEuro

Legal base & policy context

- ENISA Regulation, in particular art. 3 (Tasks)
- Directive amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (2009/140/EC), Art. 13a
- Council Resolution on "A Collaborative European Approach to Network and Information Security" (2009/C 321/01)
- European Commission's Communication on "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COM(2010) 673 final)
- European Commission's Communication on "A Digital Agenda for Europe" (COM(2010) 245 final/2
- Directive on a "Community Framework for Electronic Signatures" (1999/93/EC)
- Commission Decision on "The Publication of Reference Numbers of Generally Recognised Standards for Electronic Signature Products in accordance with Directive 1999/93/EC of the European Parliament and of the Council" (2003/511/EC)
- Commission Decision on "The Minimum Criteria to be taken into account by Member States when Designating Bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (2000/709/EC)

- Action Plan on “E-signature & E-identification” (COM(2008)798)

3.2.4 WPK 1.2: Identification and Mitigation of Threats Affecting Trust Infrastructure

Desired Impact

- At least 10 different organisations are using the conclusions of these analyses by 2014. The produced material is recognised as a neutral source of information
- At least 5 policy makers in cyber security have used the produced information
-

Description of tasks

Trust infrastructure technologies and services are considered to be of paramount importance to the trust and security of future information systems. The purpose of this work package is to identify the risks and threats this infrastructure is exposed to. Such risks/threats can emerge both from the technologies and services themselves (like bad design, improper coding, etc.) and from their improper usage. Besides the risks and threats wherever possible also the opportunities will also be identified, as this is very important to take advantage of new models for security controls and new usages of existing controls

In this work package we consider the following as trust infrastructure:

- PKI and e-Signatures at national and EU level: infrastructures and related functions and services. After the threat to Diginotar[19] and other PKI service providers, the economic analysis of this and other kind of security infrastructures needs to be analysed, and the basis for their economic suitability well defined. Strategic partnerships with those international forums dealing with security of security providers, such as the CA/Browser Forum, will be envisaged.
- National and cross-border eID schemes: eID requirements will be analysed in specific sectors, where the identity of end users is specially critical and the cost/benefit parameters are not always well evaluated, resulting in unacceptable vulnerability of the platforms:
    - E-healthcare applications
    - Financial sector
    - E-Government/ public sector
    - Web applications and application stores

Other technologies and services may be identified as appropriate on the way. The most important part of this work package, apart from analysing threats, risks and opportunities, is the assessment and communication of mitigation mechanisms and strategies. Furthermore, wherever appropriate and applicable, the impacts of the assessed risks/threats to assets of critical information infrastructures and services (see also WPK 1.1) will be considered (e.g. cloud computing, secure updates, etc.). For the implementation of such mitigation strategies existing good practice and tooling support will be taken into account. In a similar fashion as in WPK 1.1 additional issues will be taken into account where appropriate, such as:

- Economic aspects
- Assurance issues related to secure infrastructures (e.g. compliance, certification and accreditation aspects), , business continuity plans, interdependences, etc.)

The outcome of this work (risk/threat assessments and mitigation mechanisms) may be complemented by case studies, wherever appropriate, which may be tailored to a particular sector.

[19] http://en.wikipedia.org/wiki/DigiNotar

Outcomes & deadlines

The outcome of this WPK will be:

- 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)
- D2: A Good Practice Guide on dealing with these risks, where appropriate together with proposals on how to coordinate these activities with other communities
- D3: Regular reports on identified risks and opportunities in the form of "Flash Notes" and other suitable formats

Stakeholder impact

The direct beneficiaries of the results of this WPK will be Policy Makers and managers and designers of the trust infrastructure security services providers, as well as those of the technologies used to provide them to other applications and services.

- Policy Makers (Member States and EU Institutions) will be able to use the results in on going activities (e.g. policy actions, stakeholder dialogue, interaction with MS) and to support efforts to protect authentication infrastructure against identified threats. They should also profit from useful overviews of emerging threats applying to trust infrastructures and related information to increase capabilities
- Industry (private and public sector actors running parts of trust infrastructures and services) will be able to take advantage of a consolidation of existing information sources and will be better positioned to use this existing knowledge to support their own activities. This in turn should increase effectiveness of risk mitigation through knowledge transfer and capacity building. Finally, ENISA will use the results of its work to encourage industry to engage in implementation of common goals and mitigation of common risks.
- Supporting parties (standardisation institutes, research organisations) will be able to initiate research in relevant areas to contribute towards mitigation of identified emerging risks and to increase effectiveness of mitigation through knowledge transfer and capacity building.

Resources

- 15 person months
- 80 kEuro

Legal base & policy context

- ENISA Regulation, in particular art. 3 (Tasks)
- Directive amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (2009/140/EC), Art. 13a
- Council Resolution on "A Collaborative European Approach to Network and Information Security" (2009/C 321/01)
- European Commission's Communication on "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COM(2010) 673 final)
- European Commission's Communication on "A Digital Agenda for Europe" (COM(2010) 245 final/2
- Directive on a "Community Framework for Electronic Signatures" (1999/93/EC)
- Commission Decision on "The Publication of Reference Numbers of Generally Recognised Standards for Electronic Signature Products in accordance with Directive 1999/93/EC of the European Parliament and of the Council" (2003/511/EC)

- Commission Decision on “The Minimum Criteria to be taken into account by Member States when Designating Bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (2000/709/EC)
- Action Plan on “E-signature & E-identification” (COM(2008)798)

3.3 WS2- Improving pan-European CIIP & Resilience

3.3.1 Overview

Justification

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 will continue to support all in developing sound and implementable preparedness, response and recovery strategies, policies and measures to meet the challenges of a continues evolving threat environment.

EU Member States have different maturity levels in their capabilities to address cyber attacks and disruptions. ENISA, with this work stream, aims to raise the level of security across MS on CIIP issues by supporting the development of relevant capabilities in Member States. The Agency assists EU MS and the Commission to share knowledge and experience with each other on key information security issues (e.g. Smart Grids, ICS-SCADA) to develop good practices and recommendations (e.g. Governmental Clouds) that would be of mutual benefit to all, and to be better prepared to coordinate and cooperate with each other in case of cyber crisis (e.g. Crisis Management Co-operation Framework). The Agency also offers targeted assistance to EU Member States that wish to improve their security standings in certain areas (e.g. trainings on national exercises and contingency plans).

Exercising security measures for cyber incidents is now operational reality. Exercises ensure that we constantly improve and take new threats into consideration. In this work stream ENISA will continue to support MS in further developing their response and recovery capabilities via exercises. The Agency will also contribute its expertise and good practices in the global dialogue on the matter (in particular in the context of the EU-US Working Group on Cyber-security and Cyber-crime).

Supporting the Member States in the implementation of pan European regulatory measures such as article 13a (revised framework Directive for electronic communications) [20] and article 4 (ePrivacy directive) [21] requires extra effort to ensure de-facto harmonisation of measures across EU MS. In this work stream ENISA, following a soft regulatory approach, will assist the Commission in its efforts to help the NRAs in consistently implementing the Directives. The Agency will also support both NRAs and industry to agree on minimum security measures that could be widely used in the EU.

The private sector is the owner of a significant number of current critical information infrastructures. The effective co-operation between public and private sector is important for the swift implementation of ICT security measures in relevant sectors and services (e.g. priority communications). The European Public Private Partnership for Resilience (EP3R) is an important instrument in enabling such co-operation to flourish.

ENISA, through its expertise, knowledge and direct co-operation with key players in the area of CIIP, will continue to assist Member States in developing unique insights on emerging strategic, tactical and operational issues. The Agency summarises this information for the MS and Commission in the form of recommendations. It also contributes to Commission's policy and strategic initiatives (e.g. the European Strategy for Cyber Security announced by the European Commission) and monitors that actions and recommendations are properly addressed by the stakeholders.

[20] http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

Specific Policy Context

Specific policy references for this work stream are as follows:

- ENISA Regulation article 3
- Directive 2009/140/EC, Art. 13a
- Article 4 of the ePrivacy Directive
- CIIP Action Plan 2009 and 2011
- Digital Agenda 2010
- EU's Cloud Computing Strategy
- European Strategy for Cyber Security
- Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

Overall Objectives

The objectives of this Work Stream are to:

- Finalise the evaluation of Cyber Europe 2012 and initiate the organisation and management of the next Cyber Europe 2014
- support EU Commission on the implementation of the EU Strategy for Cyber Security
- 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

3.3.2 Work Packages

The following work packages constitute the Work Stream:

- WPK 2.1: Facilitating National Capability Building and Cyber crisis cooperation.
- WPK 2.2: Facilitating Public-Private cooperation.
- WPK 2.3: Improving the transparency of security incidents
- WPK 2.4: Enhancing the security of Governmental Clouds, Smart Grids and Interconnected Networks

3.3.3 WPK 2.1: Facilitating National Capability Building and Cyber Crisis Cooperation

Desired Impact

- At least 15 Member States take part in the study on National Risk Management by 2013
- At least 15 Member States request training on ENISA's NCP Good Practice Guide and Cyber Exercises Methodologies by 2014
- At least 90% of EU Member States and EFTA countries confirm their support for CE 2014
- At least 80% of Member States have established or are in the process of establishing National Contingency Plans by 2016
- At least 80% of Member States have established or are in the process of establishing National Cyber Exercises by 2016

Description of tasks

This WPK focuses on the following topics:

- Enhancing cyber contingency plans
- Organising and managing Cyber Exercises
- Training and support on NCPs and Cyber Exercises

Enhancing Cyber Contingency Plans

ENISA will continue assisting MS efforts in designing and developing national contingency plans[22]. The Agency, building on its existing work on the National Contingency Plan (NCP) Good Practice Guide, will focus on a specific part of the NCP lifecycle, namely national risk assessment and threat modelling (in co-operation with article 13 a work item). After consulting with all relevant public and private stakeholders ENISA will develop relevant good practice guide with emphasis on the 'how-to' that would help Member States to further improve their national contingency plans.

ENISA will continue supporting Member States towards the development of sound and implementable European Cyber Crisis Cooperation Framework and Procedures. The Agency will also look at the required infrastructures for cooperation, e.g. on secure communications channels, directories, etc.

Organising and Managing Cyber Exercises

In 2013 ENISA will finalise the evaluation of the second pan European exercise, i.e, Cyber Europe 2012 (CE2012) and kick off the planning for the third pan European exercise, i.e., Cyber Europe 2014 (CE2014). This exercise will build on the experienced gained in previous ones as well as their recommendations. The Agency will assess with MS whether CE 2014 could be done in coordination with the US cyber exercise Cyber Storm V.

The Agency, in the context of the EU US working group and in co-operation with MS, will exchange lessons learned with the US and contribute to the development of common co-operation procedures during crises. ENISA will also organise an international workshop on good practices for cyber exercises and update its worldwide stocktaking of existing exercises.

ENISA will further develop its methodology and technical capabilities on the organisation and management of cyber exercises. In 2013 the Agency will update the existing good practice guide on national exercise (from 2009) and enhance it by putting emphasis on creating a ready-to-use methodology with templates documents and workflows for planning cyber exercises. The Agency, in co-operation with JRC, will continue enhancing its capabilities for managing complex, distributed exercises by adding modules on scenario building and environment management.

[22] More information on ENISA's Good Practice Guide on National Contigency Plans https://resilience.enisa.europa.eu/ncp

Training and Support on NCPs and Cyber Exercises

ENISA will continue its support to MS, on how to prepare and manage NCPs and cyber exercises. Upon request, the Agency could play a more active role by offering technical expertise and advice during the preparation of NCPs or the organisation of cyber exercises. The trainings and seminars will be offered based on ENISAs portfolio of Good Practice Guides and How-To methodologies in these areas.

Outcomes & deadlines

- D1: Good Practice Guide on National Risk Assessment and Threat Modelling (report, Dec 2013)
- D2: International Workshop on Good Practices for Cyber Exercises (workshop, Sep 2013)

D3: Planning and Organising Cyber Exercises: Methodology, Templates and Toolkit (report, Nov 2013) Stakeholder impact

- EU and Member States' Public Agencies related to CIIP (such as National Cyber Security Agencies – Crisis Management Units, National Cyber Crisis Structures and Partnerships):
    - input on current level of preparedness for large-scale events and cooperation capacities
    - get an overview of pan European and International efforts in the area
    - get input, insights and recommendations for future actions in policy and technical measures
- EU Commission:
    - get insight and expert basis for current and future policy efforts in: contingency plans, cyber exercises, European Strategy for Cyber security
- CII private sector:
    - get input on current level of internal preparedness for large-scale events and inter-operator cooperation as well as public-private sector coordination
    - get insights on which requirements future actions may bring in the area of preparedness measures and continuity planning

Resources

- 25 person months
- 170 kEuro

Legal base & policy context

- ENISA Regulation article 3
- CIIP Action Plan 2009 and 2011
- EU Strategy for Cyber Security
- Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

3.3.4 WPK 2.2: Facilitating Public-Private cooperation

Desired Impact

- at least 3 position papers one for each Task Forces by end of Q4 2013,
- at least 3 national PPPs, 5 pan European associations and 15 key private companies are actively involved in the EP3R constituency by end of Q4 2013,
- 5 NRAs and 10 Cloud Computing Providers support the development of EU-wide voluntary certification schemes in the area of cloud computing
- 5 NRAs and 10 ISPs take part in in the development of the "botnets" constituency
- 7 Member States Competent authorities and 10 Private stakeholders take part in the development of the "cyber security strategy" constituency

Description of tasks

The objective of this work package is to:

- leverage EP3R as a tool to enhance public private co-operation
- provide advice and assistance to targeted stakeholder communities
- further develop the scope and impact of the European Security Month

Leverage EP3R as a tool to enhance public private co-operation

In 2012 EP3R has covered a number of key areas in the Telecommunications sector (e.g. critical ICT infrastructures, security baselines for ICT equipment and infrastructures, mutual-aid agreements, supply chain integrity).

In 2013 ENISA will continue to manage these Task Forces (TFs) with the goal of engaging more targeted stakeholders, especially smaller industry players that would broaden the views and interests the WG participants.

Building on the results of these TFs, ENISA, in consultation with relevant stakeholders, will identify topics for new TFs. Possible topics include Smart Grids and ICS-SCADA (building on the work of the Commission and ENISA), Cloud Computing for CIIP, and others. .

For each TF ENISA will identify and engage relevant public and private experts, form virtual groups of experts, and develop, when appropriate, detailed roadmaps with clear milestones and outcomes. The Agency, with support from external rapporteurs, will also arrange for regular teleconferences, organise quarterly EP3R workshops, update the EP3R portal, draft and peer review position papers, and make sure that Task Forces deliver their results according to plan. Finally, ENISA will provide advisory services to the Task Force and report to the EP3R constituencys findings and recommendations from its studies. Finally, ENISA will promote EP3R results to relevant public and private stakeholders (e.g. key industry players, Members States, and academia).

The Agency will continue liaising with existing national PPPs, cross country PPPs (e.g. Financial ISAC, EuroSCSIE, ERNCIP and others) and the EU US working group on cyber-security and cyber-crime.

Provide advice and assistance to targeted stakeholder communities

ENISA can use existing domain-knowledge as subject matter expert to assist certain public and private communities to achieve a particular goal. The Agency has decided to focus its efforts on three areas, namely:

- *Cloud Computing* – ENISA, in line with EU's Cloud Strategy recommendations, will work with NRAs and Cloud Computing Providers with the objective to create (voluntary) certification schemes which enables users to evaluate and compare in a simple manner the level of

conformance to standards, interoperability and data portability offered by providers. This should be developed into an industry-wide, uniform and simple way of describing conformity through certification.

- *Botnets* – ENISA will provide technical assistance to an EU funded[23] project that would deal with the fight against botnets. The Agency will also assist the project in the engagement of relevant public and private stakeholders, the sharing of knowledge and good practices among them, the peer review and validation of results, and the dissemination of them to targeted communities. Finally ENISA will also provide targeted recommendations to the EU on the fight against botnets and malware at large.

Cyber Security Strategies – ENISA will work with Member States competent authorities and private sector to share knowledge and good practices on the implementation of existing national cyber security strategies and their relationship to EU Cyber Security Strategy. The Agency will collect success stories and maybe failures on individual actions and share them with the community with the aim of improving our understanding about Cyber Security Strategies.

Further Development of the European Cyber-Security Month

In 2013, ENISA will continue to work together with the Member States and the Commission to further develop the European Cyber-Security Month. The approach will be to widen the number of participating Member States, to ensure sufficient focus on a number of key themes and to profile the event as a joint EU campaign with global outreach. ENISA will also seek to increase the involvement of the private sector in this initiative by working through industry representation bodies to make full use of material that has been developed already and to build upon this material when necessary.

Outcomes & Deadlines

- D1 – Management of EP3R Constituency and Task Forces (workshops/calls, Q1-Q4 2013)
- D2 - Three Position Papers (one for each Task Force) (report, Q4 2013)
- D3 – Roadmap for European Cyber-Security Month activities.

Stakeholder Impact

- Telecommunication network providers, Internet Exchange Point providers, Tier 1 providers, Vendors / Manufacturers, Security Providers, Infrastructure Operators (Data Centres, Cabling, etc.)
    - Contribute to the discussion on policies to be adopted at national and pan European level, exchange information about good practices (D4)
- NRAs, competent national authorities, ministries, European Commission
    - Understand emerging issue, interact with private sector on possible solutions, contribute to the discussion towards a common pan European strategy (D4)
- National PPPs
    - engage them in the process, help them interact with other national PPPs, share their results and good practices, understand new policy priorities (D2, D3, D4)

Resources

- 24 person months
- 150kEuro

[23] The Project is funded by EU's Competiveness and Innovation Program (CIP)

Legal base & policy context

- ENISA Regulation article 3
- CIIP Action Plan 2009 and 2011
- European Strategy for Cyber Security
- Cloud Computing Strategy
- Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union

3.3.5 WPK 2.3: Improving transparency of security incidents

Desired Impact:

- At least 20 Member States contribute to the work facilitated by ENISA on implementing and enforcing article 13a and make use of the outcomes of this work.
- 10 NRAs and/or Member State competent authorities, 10 Cloud Computing Providers take part in the study on incident reporting for cloud providers
- Support at least 2 national competent authorities in the implementation of the data breach notification scheme.
- 10 NRAs and/or Member State competent authorities, 10 ISPs, 10 Cloud Computing Providers take part in the consultation process about both article 13 a and 4

Description of tasks

This WPK focuses on the following topics:

- continue ENISA's work on article 13a and examine the feasibility of extending it to cloud providers
- continue ENISA's work on personal data breach notification
- develop synergies between article 13a and article 4

Continue ENISA's work on article 13a

ENISA will continue collecting and analysing annual, national reports of security breaches from NRAs in accordance with Article 13a of the Framework Directive on electronic communications. The Agency, in co-operation with experts from NRAs and private sector, will analyse the reports received including root causes of reported incidents, summarize statistics from the report, identify good practices and lessons learnt (especially where this can be used in exercise scenarios) and where needed make recommendations to NRAs and private sector to mitigate these threats in the future.

ENISA will also continue its work with NRAs and private sector on minimum security measures and maturity models. The Agency will assess with NRAs and private sector whether such measures could form the basis for a voluntary auditing scheme. Such a scheme is in line with article 13 a provisions and will allow NRAs to better exercise their role in auditing ISPs after a major incident. A widely accepted scheme by both NRAs and industry will, de facto, raise the level of security across ISPs and MS. In case the Commission requests ENISA to suggest technical implementing measures in line with the article 13 a provisions the Agency will use its existing guides as a basis for responding to such a request. ENISA, in close co-operation with MS competent authorities, NRAs and industry, will first evaluate and then technically assess how and under which conditions an incident reporting scheme could be implemented for cloud computing providers. ENISA's experience with Article 13 a will underpin the efforts of this study and make sure it delivers useful, practical and affordable recommendations to be used by policy makers and regulators in the context of the EU cyber security strategy.

Continue ENISA's work on personal data breach notification

ENISA will build on its work on Article 4 implementation from the previous years, particularly on the outcome of the development of technical implementation guidelines for Article 4. The reform of the regulatory framework for Electronic Communications, as well as the results of the stakeholder consultation, both on-going in 2012, will be taken into consideration. Moreover, the reform proposal of the data protection legislative framework (General Data Protection Regulation)

states that personal data breach notifications are mandatory for all data controllers. In this context, ENISA envisages to undertake activities in the following areas[24]:

- Further assist the European Commission in the implementation of the data breach notification by Competent Authorities and industry, especially in view of the reform of the regulatory framework for Electronic Communications, and the possible extension of the obligation to notify personal data breaches to all industry sectors (which is already provisioned in the General Data Protection Regulation proposal). In this goal, ENISA will need to appropriately liaise and collaborate with other stakeholders, particularly the National Competent Authorities, the Article 29 Working Party and the European Data Protection Supervisor. Also making contribution to the work of DG CONNECT in defining a list of technological protection measures that, if applied, remove the need for notification of the breaches to individuals
- ENISA will provide support to relevant competent authorities, as appropriate and in the limits of its mandate, in their preparatory activities in case of extension to other sectors of the personal data breach notification. In that respect the role of ENISA in that area is primarily one of providing advises on security measures to protect personal data.

Develop synergies among article 13a and article 4

Although there are significant differences between Article 13a and Article 4, electronic communication service providers will be obliged to implement both. Identifying potential synergies and common information security requirements for both, could, among other benefits, contribute to a reduction of the implementation cost for the private sector and simplification of the management of such incidents for the public sector.

ENISA will assess the two reporting schemes, identify common elements (e.g. parameters and thresholds) and consult relevant public and private stakeholders (e.g. NRAs, DPAs, article 29 experts, EDPS, private sector) about the most harmonised and cost efficient way of implementing their implementation. ENISA will also examine the possibility of defining a single set of guidelines, particularly targeted on the private sector. This way ENISA will aim at a more efficient and cost effective implementation which avoids any potential overlaps between both articles.

Outcomes & deadlines

- D1: Analysis of Annual 2012 Incident Reports and Recommendations for Mitigating Threats (report, Q2)
- D2: Analysis of Incident Reporting Schemes for Cloud Computing (report, Q4)
- D3: Technical Implementation Guidelines for Data Breach Notification – Update (report, Q4)

Stakeholder impact

- NRAs, DPAs and EDPS will have practical references and technical guidelines to implement the legislation.
- European Commission (DG CONNECT, HOME and JUSTICE) achieves harmonization of incident reporting, breach notifications and security measures, following international standards and can in this way forego further detailing of the legislative text.
- Industry (network providers, ISPs, cloud providers, etc.) can adopt a single framework of incident reporting/breach notification and security measures, so there is a level playing field across the EU countries and no complications for working cross borders.

[24] In view of the fact that the two legislative frameworks (i.e. ePrivacy Directive 2002/58 and reform proposal of the Personal Data Protection Framework) are still on-going at the time of drafting this Work Programme, and their provisions will obviously have a significant impact on this activity, the Agency may need to later revise the activities presented here.

Resources

- 37 person months (23 PM for article 13a and 14 PM for article 4)
- 190 kEuro

Legal base & policy context

- ENISA regulation article 3
- Commission's proposal on a European Strategy for Cyber Security
- Article 13a of the revised Framework Directive on electronic communications (Directive 2009/140 EC)
- Commission Communication on CIIP (2009 and 2011)
- ENISA regulation article 3
- Article 4 of ePrivacy Directive
- Speech by Commissioner Reding at a meeting of the Article 29 Working Party in December 2011[25]
- Reform of Data Protection legislative framework

25 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/863&format=HTML&aged=0&language=EN&guiLanguage=en

3.3.6 WPK 2.4: Enhancing the security of Governmental Clouds, Smart Grids and Interconnected Networks

Desired Impact

- 10 NRAs or other relevant government bodies and 10 Cloud Computing Providers take part in the study on governmental cloud infrastructures
- 7 Member State-NRAs and 10 Smart Grid providers take part in the development of the Smart Grids community
- 10 NRAs and 10 ISPs and IXPs take part in the study on priority data communications
- 5 Member States deploy ENISA recommendations on Governmental Cloud Infrastructures by 2015

Description of tasks

This WPK focuses on the following topics:

- securing governmental cloud computing infrastructures across the EU
- enhancing the security of Smart Grids and ICS-SCADA systems
- development of guidelines for enhancing the resilience of data communication networks

Securing Governmental Cloud Computing Infrastructures across the EU ENISA, in consultation with MS's competent authorities (e.g. NRAs, Cyber Security Agencies, ..), will take stock of existing national strategies for implementing governmental cloud infrastructures across various public sectors. The Agency will identify and assess all existing preparedness, response and recovery measures already deployed to protect assets and services of such clouds. Based on ENISA's past work and in consultation with experts from public and private sector the Agency will recommend to MS good practices on how to securely design, pilot, deploy governmental cloud infrastructures and protect them from malicious attacks and other threats. The recommendation will be categorised according to deployment models (public, private, hybrid, community) and service models (IaaS, PaaS, SaaS). Such recommendations, if consistently adopted by a critical mass of MS, could be used as public procurement guidelines and thus raise the level of security of both governmental and private cloud services across the EU.

ENISA will continue to support the Commission's cloud computing strategy including the Competitiveness and Innovation Programme (CIP) projects on Governmental and Mobile Clouds and the European Cloud Strategy projects.

Enhancing the security of Smart Grids and ICS-SCADA systems

ENISA will continue analysing existing security plans, mandatory national security measures, incident reporting mechanisms and standardisation efforts (e.g. IEC 62443, NISTIR 7628, DIN 27009) for Smart Grids. The Agency, in co-operation with the Commission, will further enhance the Smart Grids constituency by engaging experts from public and private sector and liaise with existing forums (e.g. EuroScsie, ERNCIP project). The constituency will critically asses and validate ENISA's "Minimum Security Measures for Smart Grids" and debate about the need for an IT security incident reporting scheme for smart grids and ICS-SCADA (e.g. incident management and incident severity assessment).

In consultation with MS's competent authorities and NRAs ENISA will disseminate its minimum security measures for Smart Grids (developed in 2012) to relevant operators and assist them - on their own request - towards the voluntary implementation of applicable parts. Based on the findings of this task and the feedback of the operators, ENISA will enhance and differentiate the minimum security measures accordingly. The measures, accompanied by the appropriate maturity model, could be used by NRAs as possible input for establishing national security requirements for the security of Smart Grids. This way ENISA aims to develop an acceptable scheme which can be widely deployed by both NRAs and Smart Grids operators across the EU.

ENISA will continue its co-operation with existing Industrial Control Systems' security initiatives (e.g. EuroSCSIE, ERNCIP), relevant standardisation efforts, private sector (primarily operators, ICS manufacturers, security tools providers), and regulators to implement ENISA's recommendations and good practices as they have been proposed in 2011. In that context ENISA, with support from this constituency, will contribute to the exploratory study on ICS-CERTs (in co-operation with WPK 3.2) and develop simple but yet practical guidelines on testing the security of and patching ICS-SCADA systems.

Finally, ENISA will continue supporting Commission's strategy and activities in the area of Smart Grids and ICS-SCADA.

Development of guidelines for enhancing the resilience of data communication networks

ENISA will work with national competent authorities, NRAs, IXPs and ISPs to assess the resilience of internet interconnections. Building on ENISA's work from last years, the Agency will identify possible technical means to improve availability and resilience of such interconnections. The Agency will discuss and validate its findings with all relevant stakeholders, identify possible barriers (e.g. legal) and propose to MS concrete technical guidelines on how to ensure sufficient availability and resilience of data communication networks on national level.

MS competent authorities could use such guidelines to engage ISPs and IXPs in a dialogue at national level to develop a voluntary network of ISPs and IXPs ready to assist each other during major incidents. ENISA will assist MS competent authorities in this endeavour by providing targeted advice and recommendations.

Outcomes & deadlines

- D1: Good Practice Guide for secure deployment of Governmental Clouds (report, Q3)
- D2: Guidelines on testing the security of and patching ICS-SCADA systems (report, Q4 2013)
- D3: Guidelines for enhancing the Resilience of Data Communication Networks (report, Q4 2013)

Stakeholder impact

  - Cloud Computing ENISA's recommendations for governmental clouds will allow Cloud Computing Providers to cater for different MS more easily, without having to adjust the cloud technology to different requests in different countries.
  - MS can use ENISA's recommendations in their procurement processes and switch more easily from one cloud provider to another. The adoption of these recommendations across MS will allow them to procure from service providers in other EU countries, allowing for a single digital market.

- Smart Grids and ICS-SCADA
  - ENISA's analysis and recommendations will allow policy makers in Member States and at EU level to create the right secure framework for the implementation and deployment of more efficient energy grids, and for a better incident management.
  - The raised of awareness and information sharing among stakeholders will facilitate the labour of CEOs to take investment decisions on cyber security and will enhance the network of contact points for security and incidents management.
  - Progress towards common and interoperable sets of technical security measures for different Smart Grid sub-technologies (like distribution grid operation, operation of distributed generation, smart markets, smart metering, all with different requirements). Substantial progress will allow Smart-Grid and ICS-SCADA providers and manufacturers to operate more easily across the EU-wide energy market.
  - Smart grid regulators can adopt non-technical, high-level legislation, while referring to ENISA's recommendations for implementation guidance. A single set of technical security

measures allows MS to procure technology in other EU countries and take advantage of the single EU market.

- Priority data communication
  - ISP's, IXP's will be able to use existing technology to offer services and better serve customers during crisis.
  - NRAs will identify the main elements of data communication schemes and try to deploy them at national level with the help of ENISA.

Resources

- 27,6 person months
- 180 kEuros

Legal base & policy context

- ENISA Regulation article 3
- CIIP Action Plan 2009 and 2011
- Digital Agenda 2010
- European Strategy for Cyber Security
- Cloud computing strategy
- Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union
- COM(2011) 202, Smart Grids: From innovation to deployment
- COM Recommendations on preparations for the roll-out of smart metering systems.

3.4 WS3 – Enabling communities to improve NIS

3.4.1 Overview

Justification

The aim of this WS is 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.

The most important community addressed so far by ENISA for this kind of supportive actions has been the CERT community. Whilst ENISA will continue to work with this community to improve baseline capabilities in Europe, the Agency will also complement this approach by addressing other communities that are active in improving NIS of their systems and infrastructure. These improvement guidelines will be addressed mainly to network and information systems managers.

This work stream is aimed at the providers of security services within individual organisations, such as managers of Security Operations Centres (SOC) and Information Security Officers (ISO).

Since the creation of ENISA, the Agency has been building trust between different communities, bridging the gap between the products and services offered in the market and the requirements of the users, continuously updating the information provided to those who implement security policy. The secondary aim of this work stream is to ensure that ENISA continues to be recognised as a source of expertise and assistance for NIS implementers and managers. One way to achieve this is through the development of tools to facilitate and improve international communication and interchange of security relevant information within communities sharing the same interest in different Member States.

In the Digital Agenda for Europe, one of the flagship initiatives under the Europe 2020 Strategy, the European Commission identifies and outlines policies and actions with an aim to maximize the benefits of Information and Communication Technologies (ICT). In this context, specific actions are proposed as part of the modernization of the European personal data protection regulatory framework in order "to make it more coherent and legally certain". In particular, Key Action 4 is dedicated to the "review of the European data protection regulatory framework with a view to enhancing individuals' confidence and strengthening their rights". Particular emphasis will be given to children and minors[26].

The Communication on a comprehensive approach on personal data protection in the European Union[27] has identified the enhancement of the control of the citizens over their personal data as a key objective of the comprehensive approach on data protection in the general frame of the strengthening of the rights of the individuals. In this context, the European Commission committed to examine ways of "strengthening the principle of data minimisation"; improving the modalities for the actual exercise of the rights of access, rectification, erasure or blocking of data (e.g., by introducing deadlines for responding to individuals' requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle); clarifying the so-called 'right to be forgotten', namely the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This activity will be coordinated with the application of the Data Retention Directive

[26] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0653:EN:HTML

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999D0276:20040520:EN:PDF,

[27] European Commission, A comprehensive approach on personal data protection in the European Union, Communication COM(2010) 609, 04 November, 2010, available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (last accessed on 02.03.2012)

applicable to Telecommunications Operators and recently extended to other services, addressed in Work Streams 1 and 2.

On 25/01/2012, the European Commission published its proposal for a regulation on data protection[28]. This regulation will replace the existing Data Protection Directive. It encompasses many of the concepts described above, promoting privacy by design and data protection by default while including provisions for remedies, liability and administrative sanctions in case of non-compliance. ENISA will support the implementation of the new regulation on data protection. This work will build on existing expertise in network and information security and previous work in the area of privacy and trust. Throughout its previous work ENISA has observed a clear contrast between privacy principles on the one hand and the reality of data protection practices by online service providers. Against this background the following activities aim towards supporting policy makers in the implementation of the proposed reform of data protection rules with the overall objective of increasing users' control of their data.

Furthermore, ENISA will continue its work in the area of cryptography, thereby supporting minimum requirements for data security and personal data protection across EU Member States. ENISA will promote technologies and architectures that prevent unauthorized access to personal data, unauthorized disclosure, modification, erasure, and removal of personal data.

Specific Policy Context

Specific policy references for this work stream are as follows:

- ENISA Regulation
- The Council Resolution of 18 December 2009
- Internal Security Strategy for the European Union
- CIIP Action Plan described in the Commission's communication of March 2009.
- European Commission's proposal on a comprehensive reform of data protection rules http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- Speech of Vice-President of the European Commission, EU Justice Commissioner Viviane Reding at the Independent Data Protection Authorities: Indispensable Watchdogs of the Digital Age Meeting of the Article 29 Working Party, Brussels, 7 December 2011 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/863&format=HTML&aged=0&language=EN&guiLanguage=en
- Consolidated version after the publication of Directive 2011/62/EU of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products. OJ L 174 of 1.7.2011
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001L0083:20110721:EN:PDF
- COM (2009) 149 on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"
- COM (2011) 163 on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011[29]

[28] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed on 20.02.2012)

[29] "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011 and the Council Conclusion on CIIP of May 2011 (http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf)

- COM (2006) 251 A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"
- COM(2010) 609, A comprehensive approach on personal data protection in the European Union, European Commission, Communication 04 November, 2010, available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
- Digital Agenda: http://ec.europa.eu/information_society/digital-agenda/index_en.htm
- Communication on e-commerce and other online services (2012) "A coherent framework to build trust in the Digital single market for e-commerce and online services", available at: http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm

Overall Objectives

The objective of this Work Stream is 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, the fight against cyber-crime, the protection of children and minors, etc..
- Support and enhance co-operation between CERTs and other communities.
- Develop and promote the use of training and exercise material
- Support the implementation of a pan European of Trust-marks (seals) in line with the Commission's actions in this field (i.e. Digital Agenda for Europe action 17 and e-commerce communication, COM (2011)942 action 9 trust-marks and falsified medical products) with focus in specific areas of application (e.g. online medical services, e-government services).Investigate the discrepancies between legal fundamental rights expectation and the practice in online services with regard to the principle of minimal disclosure and the 'right to be forgotten'.
- Investigate data leakage and appropriate controls for the access of data.
- In a follow up of ENISA's work in 2011 in the area of cryptography review the situation on the use of cryptographic techniques in Europe.
- Throughout this work ENISA will also identify research priorities that could be addressed in the context of the Framework Programs of EU funded R&D (FP7, FP8). At the same time, ENISA will actively contribute to the consultations organised by DG CONNECT in order to identify the R&D priorities in the area for the next call for proposals and FP8.

3.4.2 Work Packages

The following work packages constitute the Work Stream:

- WPK 3.1: Application of good practice for CERTs.
- WPK 3.2: Enabling collaborative communities.
- WPK 3.3: Enabling the Information Society.

3.4.3 WPK 3.1: Application of good practice for CERTs

Desired Impact

- Improved fast communication, response (adjusted to the threat level) and information exchange between European national/governmental (n/g) CERTs and other bodies (governmental organisations, industry and academia) adopted by a minimum of 4 Member States in 2014.
- Improved operational practices of CERTs (on-going support with best practices development) training lectured to a minimum of 20 participants of different organisations.
- Improved collaboration capabilities of n/g CERTs (continuation of 2012 work) adopted by a minimum of 4 Member States in 2014.

Description of tasks

This work package will concentrate its activities in two main streams: one addressed to keep up to date the methodologies and tools used by CERTs and security operations centres (SOC) managers, and other addressing more theoretical aspects of security and guidance:

CERT - cyber security space (methodology& tools)

In the past, ENISA has assisted the NIS community in developing methodologies and operational tools to improve the efficiency and effectiveness of their work. These tools and materials need to be updated on a regular basis, in order to support the identification of quickly evolving vulnerabilities and define associated counter measures. Examples include:

- CERT Inventory extended overview - available contacts for incident handling from other communities (CIIP and cybercrime communities, etc.) this is a fundamental tool to enable the international cooperation in case of incidents involving sites of several countries (not affordable with current resources estimation).
- n/g CERT Platform development aims to identify the requirements of a platform that will enable safe interaction and interchange of information between n/g CERTs and other CERTs within their countries. This will include:
    - Compilation of a list of atomic tasks of n/g CERTs in Europe
    - Stock taking of practice for fast administrative response procedures
- Deployment of the European Information Sharing & Alert System (EISAS) framework in Europe (based on the EISAS pilot & roadmap from 2012) using existing channels. This project has been strongly promoted by the European Commission, and its objective is to develop methodologies and tools that will allow institutions of all EU Member States to share information in order to improve the level of knowledge of end users about NIS issues like threats and vulnerabilities, and their avoidance or mitigation. The activity will take stock of the results from the EU-funded project NISHA, Network for Information Sharing and Alerting[30], which has started on 1st January 2012 as a follow up to the previously EU-funded project FISHA.

Addition to the ENISA CERT good practice library

- A good practice guide on Alerts, Warnings and Announcements (as one of the fundamental CERT services):
    - Aggregation of announcements, alerts and warnings
    - Defining and stimulating means to avoid overlapping work by exchanging information on alerts

[30] See http://fisha-project.eu/

- Incident Response Methodologies - Inventory of incident response methodologies[31] that deal with e-fraud and cyber-crime incidents such as botnets, worm infections, Scam, etc.

Outcomes & deadlines

- D1: Secure communication's platform for European n/g CERTs (Requirements & stocktaking)
- D2: EISAS – deployment in Europe (a feasibility study)
- D3: Good practice guide on Alerts, Warnings and Announcements (including an inventory of Incident Response Methodologies)
- D4: CERT Inventory; an extended overview (inventory and interactive map)

Stakeholder impact

Improvement of operations and cooperation of different communities such as: CERT, n/g CERT, CIIP, LEA and industry (SMEs).

Production and sharing of Information on cyber security, addressed to end users and SMEs.

Enhancement of operations of governmental bodies responsible for n/g CERT management.

Harmonisation of cyber security practices worldwide (focus on incident handling) - Improving the incident handling capabilities of CERTs, giving them specific guidelines on how to react in case of different types of security incidents.

Resources

- 33 person months
- 220 kEuro

Legal base & policy context

- ENISA Regulation, in particular art. 3 (Tasks)
- Council Resolution on "A Collaborative European Approach to Network and Information Security" (2009/C 321/01)
- European Commission's Communication on "Critical Information Infrastructure Protection 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'" (COM(2009) 149 final), esp. chapters 3.4.3, 5.1, 5.2 and 5.3
- European Commission's Communication on "A Digital Agenda for Europe" (COM(2010) 245 final/2), esp. chapter 2.3
- European Commission's Communication on "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COM(2010) 673 final), esp. objective 3
- European Commission's Communication on "Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'" (COM(2011) 163 final)
- European Council, "The Stockholm Programme — An Open and Secure Europe Serving and Protecting Citizens" (2010/C 115/01), e.g. par. 2.5. (Protecting citizen's rights in the information society), 4.2.3. (Mobilising the necessary technological tools), and 4.4.4. (Cyber crime)
- European Commissions' Communication on "Towards a general policy on the fight against cyber crime", COM(2007) 267 final

---

[31] This approach is similar to what several mature CERT teams offer, also these incident response methodologies were adopted by CERT-EU.

http://cert.societegenerale.com/en/publications.html

Below are White papers used by:

http://cert.europa.eu/cert/newsletter/en/latest_Publications%20and%20Newsletters_.html

- Council Framework Decision on “Attacks against Information Systems” (2005/222/JHA) and European Commission’s Proposal for a Framework Directive on “Attacks against Information Systems and Repealing Council Framework Decision 2005/222/JHA” (COM(2010) 517 final)
- Council Decision on “The Stepping up of Cross-border Cooperation, particularly in Combating Terrorism and Cross-border Crime” (2008/615/JHA)

3.4.4 WPK 3.2: Enabling collaborative communities

Desired Impact

- Improved operational capabilities of n/g CERTs (continuation of 2012 work) adopted by a minimum of 4 Member States in 2014.
- ENISA will assist at least 4 Member States in identifying and removing possible legal barriers to information sharing concerning national/governmental CERTs baseline capabilities efficiency.
- At least 20 key actors, able to act as intermediaries in the dissemination of the outcomes of the work package will be identified, covering at least 12 Member States by the end of 2013.
- Improved pan-European cooperation between CERTs and Law Enforcement Agencies (LEA) (in the area of fighting cybercrime), commitment by a minimum of 4 Member States in 2013.

Description of tasks

This work package will extend the scope of ENISA's support to the communities dealing with NIS to non-operational communities, to enable communications between CERTs, law enforcement, financial and other communities.

Communities Baseline capabilities framework

The capabilities to handle security breaches are not only a requirement for CERT community members and for this reason it is the intention of ENISA to open the target of those activities to other groups, such as Information systems managers and administrators. The activities in this area are:

- To develop a status report on the 'capabilities harmonisation with worldwide stakeholders' (improve the operational and cooperation capabilities of n/g CERTs). This activity will help n/g CERTs to define capability policies for managers of industries and SMEs, as well as public institutions. A special emphasis will be put on needed baseline capabilities to deal with incidents and other issues related to Industry Control Systems (ICS) for those CERTs which have a mandate in that area. This work item will build on previous work in the area of resilience (ICS-CERT) in 2012, and will also support current work in that area (see WPK 2.4). In addition ENISA aims at
    - Continuing the provision of support to CERT community training and to extend it to other communities (Support for TRANSITS I and II)
    - Enlarging the ENISA CERT training agenda in order to extend the target audience to more communities of IT systems managers
    - Ensuring that experience of establishing the CERT-EU is fed into training materials to benefit others trying to coordinate across multiple bodies.
- To promote brokerage activity for newly established CERTs (focus on n/g CERTs and EU accession states)
    - Facilitate wider usage of underused technologies (correlation, passive DNS, own sensor networks, client honeypot technologies, sandbox technologies, etc.)
    - Improve the understanding of legal and regulatory frameworks that CERTs have in the area of incident handling and CERT to LEA reporting, mainly in cross-border incidents.
- To 'Train the Trainers' (ENISA training portfolio developed in 2012) to also ensure that those trained are introduced to the CERT and other stakeholder communities involved in incident response.
    - Continuous cooperation with FIRST, TF-CSIRT, EU CERT, EGC, APCERT, NCIRC, TRUSTED INTRODUCER, APWG, and other relevant stakeholders)
    - Hosting CHICHT service

Enabling collaborative communities

The following activities are designed to enable ENISA to facilitate the establishment of and to maintain contacts between CERTs, LEAs and other communities:

- Building an expert group on practical solutions for information sharing and international incident handling process within current legal frameworks
- Developing a Good practice Guide on the practical implementation of the "directive on attacks against information systems and repealing Council Framework Decision - 2010/0273(COD)"
- Managing the 8th Annual CERT workshop – International Incident handling (legal perspective and operational contacts, etc.)
- Disseminating the CERT exercise material – cybercrime scenarios
- ENISA will seek contact and collaboration with the newly established European Cyber Crime Center (ECCC) in Europol, and thereby extend its already very fruitful cooperation with Europol. This collaboration will be restricted to information exchange and exchange of good practice.

European Strategy for Cyber Security

- Coordinating ENISA's contribution to the work in this area led by the European Commission.

Outcomes & deadlines

- D1: Good practice guide on the practical implementation of the "directive on attacks against information systems"
- D2: 8th Annual CERT workshop report (public version)
- D3: CERT exercise material - extended – cybercrime scenarios (handbook and toolset)
- D4: New version of Baseline capabilities framework – international harmonisation (Status report on capabilities harmonisation with worldwide stakeholders) and appropriate ICS-CERT capabilities
- D5: CERT training support (TRANSITS and ENISA training portfolio activities)
- D6: Good practice guide on harmonisation and implementation of legal frameworks for information sharing and international incident handling process

Stakeholder impact

The benefit to stakeholders of this work package will be:

- n/g CERTs will benefit from the brokerage and cooperation capabilities enhancement.
- LEA units and managers of industries and SME will be able to participate in training courses organised by ENISA or supported by ENISA through provision of material or training trainers.
- Members of Financial Institutions CERTs and IT managers will also benefit from the contributions of ENISA in this WPK through participation on for a specially interesting to them, such as APWG (Anti-Phishing Working Group).

The benefits will be realised mainly as training and capability enhancement actions specially tailored for those communities.

Resources

- 34 person months
- 225 kEuros

Legal base & policy context

- ENISA Regulation, in particular art. 3 (Tasks)

- Council Resolution on “A Collaborative European Approach to Network and Information Security” (2009/C 321/01)
- European Commission’s Communication on “Critical Information Infrastructure Protection ‘Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience’” (COM(2009) 149 final), esp. chapters 3.4.3, 5.1, 5.2 and 5.3
- European Commission’s Communication on "A Digital Agenda for Europe" (COM(2010) 245 final/2), esp. chapter 2.3
- European Commission’s Communication on “The EU Internal Security Strategy in Action: Five steps towards a more secure Europe” (COM(2010) 673 final), esp. objective 3
- European Commission’s Communication on “Critical Information Infrastructure Protection ‘Achievements and next steps: towards global cyber-security’” (COM(2011) 163 final)
- European Council, “The Stockholm Programme — An Open and Secure Europe Serving and Protecting Citizens” (2010/C 115/01), e.g. par. 2.5. (Protecting citizen’s rights in the information society), 4.2.3. (Mobilising the necessary technological tools), and 4.4.4. (Cyber crime)
- European Commissions’ Communication on “Towards a general policy on the fight against cyber crime”, COM(2007) 267 final

3.4.5 WPK 3.3: Enabling the Information Society

Desired Impact

- Survey of security certification practice in at least 5 Member States to identify best practice that could be applied for privacy certification/trustmarks;
- Recommendations for best practice on data security of personal data/the use of cryptographic techniques for eGov services in Europe based on inputs from at least 5 Member States;
- Supporting the EC DG CONNECT following its proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market, involving at least 5 relevant stakeholders from public and private sectors.

Description of tasks

The main objective of this work package is to increase the trust in the online services and the infrastructure supporting them, mainly when these infrastructures are outside EU. The ultimate goal is to better inform users and customers about the evolvements in the digital world, keeping a global perspective and accounting the context beyond EU MS in borderless Internet.

On 11 January 2012, the European Commission adopted the Communication on e-commerce and other online services[32] announced in the "Digital Agenda"[33] and the "Single Market Act"[34] . The adopted Communication presents 16 action points organized in 5 priorities for stimulating economic growth and employment using online services. Three of these priorities are:

- consumer information and protection – including personal data protection according to the revised data protection acquisition. Action 9 of the communication includes “ensure adequate protection for patients purchasing medicinal products online by contributing to the creation of trustmarks” according to the recent directive on Directive 2011/62/EU of 8 June 201135 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use. These trustmarks could be useful in the area of e-commerce applications.
- payments and delivery systems – by supporting mutual recognition of electronic identification and authentication and on electronic signatures and, as mention in action 10, by developing a strategy for “increasing the level of security of payments and data protection”,
- abuses and disputes – by also focusing on strengthening security, ensuring that the internet security mechanisms are in place and are able to cope effectively with cyber-attacks and technical failures, addressed in action 13, where an overall strategy on internet security in Europe is foreseen.

[32] http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm

[33] http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[34] COM/2011/0206 final

[35] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001L0083:20110721:EN:PDF – consolidated version after the publication of Directive 2011/62/EU of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products. OJ L 174 of 1.7.2011.

Consumer information and protection

Supporting these activities is essentially a follow up of ENISA's work under WP2012. The European Commission adopted in January 2012[36] a proposal for a regulation on data protection that will replace the existing Data Protection Directive. The proposal for the new Regulation contains specific provisions relevant to certification, data protection seals and marks. In 2013 ENISA will support related activities relevant to certification and on trustmarks (privacy seals) of the European Commission and JRC which are planned for 2013-2014. ENISA can contribute to this area by identifying best practice from security certification and security seals that could be used and applied also to privacy certification. Furthermore, ENISA could focus on specific areas of application such as online medical services for citizens or eGov services which will have to comply as well with the new personal data protection legal requirements.

The Agency will support the European Commission in its efforts in the area of Identity Management. EU funded projects like IDABC and STORK prepared the ground for further work. Possible subjects are trusted eID, eAuthentication mechanisms (where ENISA already delivered valuable studies in the previous years), eID certification schemes and eSignatures. The Agency will continue to provide guidelines and recommendations, and support the implementation of proposed solutions at the Member States level.

Securing personal data in online environments

The correct use of cryptography minimises certain threats and secures e-government services. At the end of 2011 ENISA published a study examining the cryptographic documents and specifications defined by European Union Member States related to the encryption of unclassified information stored and transmitted by e-government services. ENISA considers that significant benefits are expected from an EU-wide initiative to specify a common minimum standard for cryptography of unclassified data in e-government services. From a long-term perspective this would not only ensure a certain level of protection for all EU citizens, but also would simplify the exchange of government data between MS – which becomes increasingly important with the increasing mobility of citizens. Providing these guidelines publicly, other stakeholders will benefit from such an initiative, for instance could bring economies of scale to the commercial market outside e-government services.

ENISA will revise and update the study on the use of cryptographic techniques in Europe focussing on specific areas where data security is needed to protect personal data of the citizens[37]or on the requirements for new techniques required by new applications (e.g. cloud computing, smart phones etc.).

The aim of the European Directive 1999/93/EC[38] on a community framework for electronic signatures was the legal recognition of electronic signatures. Assessing the need for secure and seamless electronic transactions as well as the shortcomings of the Directive, the European Commission (EC) has adopted on 4.6.2012, a proposal for a Regulation[39] on electronic identification and trusted services for electronic transactions in the internal market.

---

[36] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed on 20.02.2012)

[37] i.e. data security in the implementation of data retention reform. ENISA is supporting, on request, EC DG HOME in this area.

[38] http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett

[39] http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

In 2012 ENISA has contributed to the discussions on the proposed regulation by assessing the feasibility of the introduction of an obligation of reporting security breaches by the trust service providers to the competent bodies. In 2013, due to its role in the EU ICT security landscape, the Agency will follow up this subject by investigating good practices for security of electronic identification systems, good security practices of trust service providers and supervisory authorities, and will analyse the security practices in eID systems and initiatives, as well as the findings of the Large Scale Projects in relation to security. An expert workshop is also foreseen to validate the findings.

On 10-11 October 2012 ENISA organised the first Annual Privacy Forum (APF'2012) http://privacyforum.eu/ in partnership with DG CONNECT, -Cyprus Presidency of the Council of the EU and the University of Cyprus. The main objective of the APF, is to establish a forum fostering the exchange of information and experiences between the research and academic communities, and the EU policy and industry representatives. The response to the organisation of the first edition of the conference in 2012 indicates that APF can become an established reference event in the area of privacy putting emphasis on the need to bring together the policy and research communities.

At the time of preparing the Work Program text the final evaluation of APF'2013 is not yet concluded. In this light, it is not yet fully confirmed whether an edition of APF will be organised in 2013. Experience from APF'2012 clearly indicates that the collaboration model between DG CONNECT and ENISA in the joint organisation of APF is the way forward. In this light the decision to proceed with APF in 2013[40] would have to wait first for the conclusion of APF'2012 and its evaluation.

Outcomes & deadlines

- D1: Supporting EC activities in the implementation of trustmarks. Identifying best practice from security certification that could be deployed for privacy certification and trustmark (report, Q4)
- D2: Recommendations for best practice on data security of personal data/the use of cryptographic techniques for eGov services in Europe (report, Q4)
- D3: good practices for security of electronic identification systems (report, Q4)
- D4: eID workshop (event, Q3)
- D5: Dissemination activity (e.g. panel session) focusing on the work in the area of privacy and trust (event, Q1-Q3)

Stakeholder impact

- Supporting the development of clear guidelines for service provider in the light of the new data protection Regulation in close collaboration with DPAs, NRAs, Article 29 and EDPS, European Commission (DG JUS, DG CONNECT and DG HOME), covering topics such privacy seals, personal data protection – data security, etc.
- Supporting the implementation of digital agenda, data protection Regulation for Industry Providers (network operators, service providers) etc.
- Harmonisation of practices regarding data security and data protection across Member States and service providers (i.e. minimum security requirements).

Resources

- 29 person months
- 125 KEuro

[40] Another possible alternative, with reduced demands in terms of resources is to maintain APF but with bi-annual periodicity.

Legal base & policy context

- ENISA regulation article 3
- European Commission's proposal on a comprehensive reform of data protection rules http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- Speech of Vice-President of the European Commission, EU Justice Commissioner Viviane Reding at the Independent Data Protection Authorities: Indispensable Watchdogs of the Digital Age Meeting of the Article 29 Working Party, Brussels, 7 December 2011
- http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/863&format=HTML&aged=0&language=EN&guiLanguage=en '…I also want to extend data breach notifications to all sectors. Data controllers will have to report security breach incidents to data protection authorities and to the individuals whose personal information has been compromised. I intend to strengthen data protection officers in the public sector, in large companies and in companies doing risky processing. They will be your point of contact.
- European Commission, A comprehensive approach on personal data protection in the European Union, Communication COM(2010) 609, 04 November, 2010, available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
- Consolidated version after the publication of Directive 2011/62/EU of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products. OJ L 174 of 1.7.2011.
- Digital Agenda http://ec.europa.eu/information_society/digital-agenda/index_en.htm
- Communication on e-commerce and other online services (2012) "A coherent framework to build trust in the Digital single market for e-commerce and online services", available at: http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm
- The proposal for a Regulation "on electronic identification and trusted services for electronic transactions in the internal market" adopted by the Commission on 4th June 2012, available at: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm .

3.5 Summary of core operational activities

WS1	Evolving Risk Environment & Opportunities	Budget Line	Budget	Person Months
WPK 1.1	Identification & mitigation of threats affecting Critical Information Infrastructure	3620	80.000	15,0
WPK 1.2	Identification & mitigation of threats affecting Trust Infrastructure	3620	80.000	15,0
	Totals		**160.000**	**30,0**
WS2	**Improving Pan-European CIIP & Resilience**	**Budget Line**	**Budget**	**Person Months**
WPK 2.1	Cyber crisis cooperation	3610	170.000	25,0
WPK 2.2	Facilitating Public-Private cooperation	3610	150.000	24,0
WPK 2.3	Improving transparency of security incidents	3610	190.000	37,0
WPK 2.4	Enhancing the security of Governmental Clouds, Smart Grids and Interconnected Networks	3610	180.000	27,6
	Totals		**690.000**	**113,6**
WS3	**Enabling Communities to Improve NIS**	**Budget Line**	**Budget**	**Person Months**
WPK 3.1	Application of good practice for CERTs	3600	220.000	33,0
WPK 3.2	Enabling collaborative communities	3600	225.000	34,0
WPK 3.3	Enabling the information society	3600	125.000	29,0
	Totals		**570.000**	**96**
Total			**1.420.000**	**239,6**

TCD Missions		440.000	

Summary of Core Operational Activities with deliverables

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
D2	A Good Practice Guide on dealing with these risks, where appropriate together with proposals on how to coordinate these activities with other communities
D3	Regular reports on identified risks and opportunities in the form of “Flash Notes” and other suitable formats

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)
D2	A Good Practice Guide on dealing with these risks, where appropriate together with proposals on how to coordinate these activities with other communities
D3	Regular reports on identified risks and opportunities in the form of "Flash Notes" and other suitable formats
WS2	**Improving Pan-European CIIP & Resilience**
WPK 2.1	Cyber crisis cooperation
D1	Good Practice Guide on National Risk Assessment and Threat Modelling
D2	International Workshop on Good Practices for Cyber Exercises
D3	Planning and Organising Cyber Exercises: Methodology, Templates and Toolkit
WPK 2.2	Facilitating Public-Private cooperation
D1	Management of EP3R Constituency and Task Forces (workshops/calls
D2	Three Position Papers (one for each Task Force)
D3	Roadmap for 'European Cyber-Security Month' activities
WPK 2.3	Improving transparency of security incidents
D1	Analysis of Annual 2012 Incident Reports and Recommendations for Mitigating Threats
D2	Analysis of Incident Reporting Schemes for Cloud Computing
D3	Technical Implementation Guidelines for Data Breach Notification – Update
WPK 2.4	Enhancing the security of Governmental Clouds, Smart Grids and Interconnected Networks
D1	Good Practice Guide for secure deployment of Governmental Clouds
D2	Guidelines on testing the security of and patching ICS-SCADA systems
D3	Guidelines for enhancing the Resilience of Data Communication Networks
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)

D2	EISAS – deployment in Europe (a feasibility study)
D3	Good practice guide on Alerts, Warnings and Announc333ements (including an inventory of Incident Response Methodologies)
D4	CERT Inventory; an extended overview (inventory and interactive map)
WPK 3.2	Enabling collaborative communities
D1	Good practice guide on the practical implementation of the "directive on attacks against information systems"
D2	8th Annual CERT workshop report (public version)
D3	CERT exercise material - extended – cybercrime scenarios (handbook and toolset)
D4	New version of Baseline capabilities framework – international harmonisation (Status report on capabilities harmonisation with worldwide stakeholders) and appropriate ICS-CERT capabilities
D5	CERT training support (TRANSITS and ENISA training portfolio activities)
D6	Good practice guide on harmonisation and implementation of legal frameworks for information sharing and international incident handling process
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
D2	Recommendations for best practice on data security of personal data/the use of cryptographic techniques for eGov services in Europe
D3	Good practices for security of electronic identification systems
D4	eID workshop
D5	Dissemination activity (e.g. panel session) focusing on the work in the area of privacy and trust

4 Operational Horizontal Activities

4.1 Stakeholder activities

4.1.1 Aligning to the Policy Environment

No organisation operates in a vacuum, least of all, a European agency. In aligning to the policy alignment, ENISA needs to take account of developments at a European level, with the Parliament, Council and Commission, at the level of Member States, where individual countries make crucial contributions to ENISA's work, and, increasingly, at a wider, global level.

The Agency's ability to foresee, respond to, and help shape NIS policy will remain a crucial focus for 2013. ENISA's structure, with a Management Board that includes representatives of Member States, a Permanent Stakeholder Group that represents the ITC industry, academia and consumers and a network of National Contact Officers (also known as National Liaison Officers) provides a robust, flexible structure for staying attuned to policy developments, and disseminating good practice that can help to form policy.

In the year ahead, ENISA will work to consolidate its capabilities in policy alignment, using its existing structures, and seeking new ways in which it can react to and shape policy, such as developing earlier and deeper engagement with stakeholders when formulating plans for reports and activities.

4.1.2 Management Board, PSG Secretariat and NCO/NLO network

This covers all activities that are required to support ENISA's formal bodies, the Management Board (MB) and the Permanent Stakeholders Group (PSG) in their functions.

For the MB, two formal meetings will be organised during 2013 and joint informal meetings of sub-groups will be held with the PSG as appropriate. The existing electronic newsletter will be continued throughout 2013, as will support for the MB Portal.

For the PSG also, two formal meetings will be organised.

ENISA will continue to explore other ways of supporting these two communities in the most effective way, including the possible use of new technologies and modifications to existing processes as required.

In order to make the most of its stakeholder community and also to ensure that it server the latter as effectively as possible, ENISA will aim to involve stakeholders in concrete activities wherever possible.

The National Contact Officers (NCO) is an extension of the National Liaison Officers (NLO). The NLO is extended with contact points from Governmental CERTs and Regulatory Bodies/Agencies.

A single point of contact by NLOs in MS will be maintained for those officials acting in direct support of (or who themselves are) members of the ENISA Management Board.

ENISA envisages ad hoc meetings with National Contact Officers on particular topics of interest and to host 1 meeting with them in 2013.

4.1.3 EU Relations

The Agency will continue to develop and enhance relations with EU Institutions and Bodies. In particular, ENISA will seek to ensure that other European institutions and bodies are aware of the work that the Agency is carrying out and are liaising with the Agency in the most effective way.

ENISA will undertake the analysis and review of EU policy acts when requested to do so and on its own initiative when this is in the interest of its stakeholders.

Developing and maintaining a network of key actors, advocacy and regular interaction with ENISA's relevant stakeholders in the EU Institutions is highly importance in order to raise the Agency's profile as such and, finally, to 'enhance the levels of security in Europe'. ENISA will therefore continue to maintain visibility in debates relating to NIS by participating in high-level events.

Finally, ENISA shall provide advice and assistance, as stated in its founding regulation, to the EU Institutions regarding relevant NIS policy issues.

4.2 Project Support Activities

4.2.1 Dissemination Activities

ENISA considers dissemination as a 'horizontal activity' in the sense that this usually takes place within the particular work packages defined by the work plan. There is a need however to coordinate the messages being passed in the different subject areas.

The objectives of this project support activity are as follows:

- Ensuring the coherence at the Agency level of dissemination initiatives that take place within individual work packages.
- Promoting the use of technology to achieve a greater impact.

Ensuring coherence of dissemination activities

This task involves liaising regularly with the teams that implement the different work packages of the work programme and ensuring that the messages that are being passed are coherent from an agency perspective.

Promoting the use of technology to achieve a greater impact

The aim of this work is to identify technology channels that could be useful for supporting dissemination activities and to support their use in the various activities that ENISA undertakes. Particular attention will be given to new media technologies (e.g. social networks, etc.).

4.2.2 Tracking Standards

ENISA has established collaboration agreements with a number of standardisation bodies. This collaboration was continued in 2011 through the participation in meetings of TISPAN WG7 and collaboration in the elaboration of a study on ontology and taxonomies of resilience. At the same time contacts with ISO SC27 were launched (WG5 – Identity management and privacy technologies) and ITU SG17.

In 2012, ENISA contributed actively to the newly formed CEN-CENELEC-ETSI Cyber Security Coordination Group (CSCG) also hosting the 4th meeting of the group in December 2012. In 2013, ENISA will continue contributing to CSCG. At the same a co-operation agreement with CEN-CENELEC was concluded (in the lines of the existing Memorandum of Understanding with ETSI). In the context of these co-operation agreements with CEN-CENELEC and ETSI and as part of this work, the Agency will seek out synergies with the work programme and involve standards bodies in the different work packages in as far as this is appropriate. The work in this area will ensure that any activities associated with standards and contained in the different work packages will be correctly coordinated at the Agency level.

4.3 Public Affairs Activities

4.3.1 Public Relations

To deliver its mission to enhance network and information security for Europe, ENISA must be able to communicate effectively with the general public and specific target groups. These range from politicians and leaders of industry, to academic research institutions and end-users of ICT hardware and software. ENISA's ways of engaging with these groups must reflect their differing needs and expectations of the Agency. In 2013, ENISA will continue to refine its existing capabilities, and develop new avenues for continuing the dialogue with its stakeholders.

Core public relations activities, such as press and media releases, ENISA workshops and conferences and publications will continue. However, the emphasis will be increasingly on smaller, flexible events and activities that take the message to the audience at a local level. This will build on work piloted in 2012.

4.3.2 ENISA Digital Communications

ENISA's web site continues to be the Agency's most important communications channel, and in 2013 it will be further developed to build on the redesign that took place in 2012. The new look web site enables users to locate the information they want , quickly and easily, whether they are academics seeking ENISA's latest research papers, or more casual browsers, who have "Googled" their way to the site looking for tips on safer Internet surfing.

While the focus of the redesign is on accessibility, "behind-the-scenes" developments include a greater ability to gather and analyse data on which of ENISA's web pages and reports are receiving the greatest number of hits, and search engine optimisation, to help people find ENISA's information more easily. The tagging and ENISA's reports has also been revised, again to improve search functions. Work on enhancing these developments will continue throughout 2013. ENISA's web site links with other NIS organisations will also be increased, as will the amount of information that the Agency makes available in French, German and Greek, though its "landing pages" in these languages.

Web portal "mini-sites" already serve ENISA's various special-interest user communities, and ENISA will continue to seek new ways to customise its messages and delivery methods to users' requirements. From 2012, these have included a presence on social media sites, such as Facebook, LinkedIn and Twitter, and 2013 will see the Agency making ever greater use of these opportunities to engage directly with its stakeholders.

4.3.3 Publications & Brand Material

ENISA's publications and brand material are a crucial part of how it communicates its NIS messages. Along with the web site, they are the "shop window" for ENISA's activities. In recognition of their importance, in 2012, the Agency carried out a full redesign for all of its published and branded material, including the ENISA General Report, published annually, its expert reports on NIS topics and its exhibition and promotional material. Working with this fresh brand identity, the Agency in 2013 will continue to increase its range of publications and brand material that are accurately targeted at its differing audiences.

Reflecting environmental concerns and the need to deliver quickly and flexibly, ENISA will continue to publish most of its material electronically, though the ENISA web site, and also make this available through web links to NIS organisations in Member States and other countries outside the EU.

An ENISA electronic newsletter, re-launched to great success in 2012, as a successor to the ENISA Quarterly Review, will continue to be developed in 2013, to provide timely, accurate information on ENISA and NIS, with live links to take readers to more information.

4.3.4 Spokesman and Media Relations

The media provide ENISA with an opportunity to reach many more people than it can through direct means. In 2013, ENISA will continue to issue media releases (in different EU languages) to press, radio, television and web-based media organisations. These include general media, and specialist NIS publications and web sites, with ENISA monitoring the uptake and impact of resulting media coverage.

As the Agency's primary media contact, the Spokesman will continue to ensure that the media are aware of ENISA's latest work. This includes both speaking directly for the Agency, and organising press conferences and briefings with journalists as part of ENISA's planned communication calendar. A number of special briefings are planned for national media in Member States, and specialist NIS and ICT media.

4.3.5 Events

ENISA's activities Range from special events where NIS experts and policy makers are invited to discuss the "big issues" around network and information security, to highly specialised workshop meetings to explore issues around such things as legislation, or specific security risks. ENISA's 2013 programme features a number of "roadshow" events, where the Agency will capitalise on its links with Member States and other EU bodies to deliver tightly focused NIS messages to specific audiences. A keynote event for stakeholders is planned for Brussels in the autumn of 2013.

4.3.6 Internal Communication

In 2013, ENISA will need to operate eve more flexibly in order to meet the needs of its stakeholders in all Member States. Ensuring that shared understanding of objectives and business needs is ever more crucial with a workforce that is not all working from the same location. Throughout 2011 and 2012, ENISA's internal communications focused on ensuring that the Agency's personnel could share in a common culture, not just knowing what the Agency's role is, but also understanding why it exists, and how ENISA fits into the wider European Union picture. This work continually needs to be evaluated and updates, as the context develops, and personnel change. To ensure that information can be is shared and updated quickly, ENISA's internal communications activities include weekly staff meetings and an intranet system, accessible remotely from any location. Staff in the Agency's Athens office participate in staff meetings via a secure, fully interactive audio-visual web connection.

The 2013 Internal Communications programme includes work to refresh and update ENISA's shared values and ways of working, as well as teambuilding events.

4.4 Summary of Operational Horizontal Activities

SR	Stakeholder Relations	Budget Line	Budget	Person Months
SR1	Alignment to the policy environment	N/A	N/A	3,0
SR2	MB & PSG secretariat, NCO/NLO network	3001	180.000	9,6
SR3	EU relations	N/A	N/A	11,6
	Totals		**180.000**	**24,2**
PS	**Project Support Activities**	**Budget Line**	**Budget**	**Person Months**
PS1	Dissemination activities	N/A	N/A	0,0
PS2	Tracking standards	N/A	N/A	6,0
	Totals		**0**	**6,0**
PAU	**Public Affairs**	**Budget Line**	**Budget**	**Person Months**
PAU1	Public relations	N/A	N/A	7,0
PAU2	Digital communication	3220	131.000	9,0
PAU3	Publications & brand material	3240	65.000	4,0
PAU4	Spokesman & media relations	3210	49.000	9,0
PAU5	Events	3200	10.000	4,0
PAU6	Internal communication	3011	2.000	4,0
	Totals		**257.000**	**37,0**
Total			**437.000**	**67,2**

	PAU Missions		70.000	

5 IT & Facilities Management

5.1 Introduction

ITFMU is responsible for the delivery of agency-wide services for IT, for Safety & Security and for Facilities Management.

5.2 Activities

Activities related to IT include help desk, operations and monitoring, services management and infrastructure management, solutions and development.

Facilities Management activities include building maintenance, inventory management, transport and delivery services and meeting services.

Safety and Securities activities include physical and personnel security, health and safety, emergency and contingency plans.

5.3 Budget

Activity	Unit	Budget line	Budget	Person Months
IT	ICT Services	Chapter 23	305.000	38,4
FM	Facilities Management Services	2002	7.000	9,6
		2003	20.000	
		2004	50.000	
		2005	18.000	
		2100	5.000	
		2110	15.000	
		2121	2.000	
		2122	2.000	
		2123	5.000	
SS	Safety & Security Services	2006	15.000	9,6
		2007	140.000	
Total			**584.000**	**57,6**

ITFMU Missions		10.000	

6 Administration activities

6.1 Overview

The Administration Department consists of two main sections Finance, Accounting & Procurement (FAP) and Legal & Human Resources section (LHR). In 2013 the latest, a Head of Administration should take up her/his duties and continue with the of the reforms started by the Executive Director in 2012 regarding the implementation of streamlining procedures and working practices.

Moreover, a particular stress is put on staff motivation and individual performance monitoring. The Administration Department takes all the necessary actions in order to ensure that the management of the Agency is in line with EU institutions' established standards.

The Administration is responsible for the management of the budget appropriations of Title 1 – Staff costs (€ 5.453.541,70), part of Title 2 – Administrative expenditure (books & subscriptions, stationery & office supplies, postage, and bank charges, totalling €45.000), and the cost of translations (BL 3230 - €21.011), ED meetings (BL 3005 - €2.000) and other operational meetings (BL 3021 - €3.000) funded by Title 3 – Operational expenditure

6.2 Activities

The Administration Department activities for 2012 are summarised in the table below:

Activity Ref.	Activity Description	Budget Line	Budget	Person Months
ADA 0	General Management	3005 3021	2.000 3.000	10,6
ADA 1	General Administration activities, including work carried out in the Directorate: Management, meetings, secretarial support, Internal Control Coordination (ICC), translations	2130 2200 2201 2203 2210 3230	10.000 15.000 15.000 3.000 2.000 21.011	19,2
ADA 2	Finance, Accounting & Procurement activities, including processing of financial transactions, finance helpdesk, budget preparation and monitoring, missions management and relations with Hellenic Authorities	2210	2.000	86,4
ADA 3	Legal & Human Resources activities, including legal advice, rights and obligations management, recruitment and training	Title 1	5.453.542	32,6
Total			**5.524.553**	**148,8**

ADMIN & Directorate Missions		64.000	

7 APPENDIX A Activities and corresponding Budget Lines in Statement of Estimates 2013 (Budget 2013)

Statement of Estimates 2013		**Work Programme 2013**			
Budget Line	Heading	WP ref.	Title	Amount	Totals
3001	Meetings of Official Bodies	SR2	MB & PSG secretariat, NCO/NLO network	180.000	180.000
3005	Executive Director Office Meetings	ADA 0	General Management	2.000	2.000
3011	Entertainment and Representation expenses	PAU 6	Internal communication	2.000	2.000
3016	Missions	MISS	Missions of all staff	584.000	584.000
3021	Other Operational meetings	ADA 0	General Management	3.000	3.000
3200	Conferences and Joint Events	PAU 5	Events	10.000	10.000
3210	Communication activities	PAU 4	Spokesman & Media relations	49.000	49.000
3220	Web-Site Development	PAU 2	Digital Communication	131.000	131.000
3230	Translations	ADA 1	General Administration activities	21.011	21.011
3240	Publications	PAU 3	Publications & brand material	65.000	65.000
3600	Stakeholders' collaboration	WPK3.1	Application of good practice for CERTs	220.000	570.000
		WPK3.2	Enabling collaborative communities	225.000	
		WPK3.3	Enabling the information society	125.000	
3610	NIS Policy	WPK2.1	Cyber crisis cooperation	170.000	690.000
		WPK2.2	Facilitating Public-Private cooperation	150.000	
		WPK2.3	Improving transparency of security incidents	190.000	
		WPK2.4	Enhancing the security of Governmental Clouds, Smart Grids and Interconnected Networks	180.000	
3620	NIS Technology	WPK1.1	Identification & mitigation of threats affecting Critical Information Infrastructure	80.000	160.000
		WPK1.2	Identification & mitigation of threats affecting Trust Infrastructure	80.000	
	Grand total - Title 3			**2.467.011**	**2.467.011**

8 APPENDIX B : Operational Activities 2013 (Activity Based Budgeting)

OPERATIONAL ACTIVITIES 2013	Operational HR in person/years (Note 1)	Salary Costs Operational HR in EUR (Note 2)	Operational Expenditure in EUR (Note 3)	Overheads in EUR (Note 4)	Total Activity Cost in EUR
WS1 - Evolving Risk Environment & Opportunities	**3,1**	**261.942**	**160.000**	**213.752**	**635.694**
WS2 - Improving Pan-European CIIP & Resilience	**11,8**	**991.886**	**690.000**	**809.409**	**2.491.295**
WS3 - Enabling Communities to Improve NIS	**10,0**	**838.214**	**570.000**	**684.008**	**2.092.221**
SR - Stakeholder Relations	**2,5**	**211.300**	**180.000**	**172.427**	**563.727**
PS - Project Support Activities	**0,6**	**52.388**	**0**	**42.750**	**95.139**
PAU - Public Affairs	**3,9**	**323.061**	**257.000**	**263.628**	**843.689**
Missions	**0,0**	**0**	**584.000**	**0**	**584.000**
Management & Support activities (Note 5)	**8,0**	**670.571**	**26.011**	**547.206**	**1.243.788**
Total (Note 6)	**40,0**	**3.349.361**	**2.467.011**	**2.733.180**	**8.549.553**

Note 1 - The Operational Human Resources consist of the number of ENISA Staff and Seconded National Experts (SNE) directly involved in the implementation of the relevant activities.

Note 2 - The salary costs of Operational Human Resources consists of the cost of ENISA Staff and SNE directly involved in the implementation of the activities.

Note 3 - The Operational expenditure is the direct cost attributed to each activity, provided for in WP and the Statement of Expenditure 2013.

Note 4 - Overheads include all costs which are indirectly involved in the implementation of WP 2013, such as salary costs of non-operational staff, rent, and running costs (e.g. Office supplies).

Note 5 - Management & Support activities include the budget allocated to ED meetings (BL 3005), Other operational meetings (BL 3021) and Translations (BL 3230) of the Agency.

The HR allocated to Management & Support activities includes the ED staff (2), the Head of Department and the Heads of Units of TCD, the Head of PAU, and the Quality Control Advisor.

Note 6 - The total human resources in person/years figure (40) differs from the actual man power for the year 2013 (44 posts) due to recruitment planning, which affects new staff availability,

as well as part time working schemes of existing staff.