enisa
European Network and Information Security Agency

WORK PROGRAMME 2011

Securing Europe's Information Society

Contents

ACRONYMS 4

1. EXECUTIVE SUMMARY 6
1.1 Background 6
1.2 Structure 7
1.2.1 Work Streams 7
1.2.2 WS1 - ENISA as a facilitator for improving cooperation 7
1.2.3 WS2 - ENISA as a competence centre for securing current & future technology 8
1.2.4 WS3 - ENISA as a promoter of privacy, trust and awareness 8
1.2.5 Stakeholder engagement activities 8
1.2.6 Public Affairs activities 9

2. INTRODUCTION 10
2.1 Relation to the previous work programme 10
2.2 Policy context 10
2.2.1 Background 10
2.2.2 The CIIP Action Plan 10
2.2.3 The Electronic Communications Regulatory Framework 11
2.2.4 The Council Resolution 11
2.2.5 The Digital Agenda 11
2.2.6 The Commission proposal on the future of ENISA 12
2.3 Key challenges 12
2.3.1 Fostering a proactive NIS community 12
2.3.2 Assisting Member States in implementing secure services 13
2.3.3 Promoting uptake of ICT by the citizen through an enhanced framework for privacy and trust 13
2.4 ENISA's role 13

3. WORK STREAMS 14
3.1 WS1 : ENISA as facilitator for improving cooperation 14
3.1.1 WPK 1.1: Supporting Member States in implementing article 13a 16
3.1.2 WPK 1.2 : Preparing the Next Pan-European Exercise 18
3.1.3 WPK 1.3: Reinforcing CERTs in the Member States 20
3.1.4 WPK 1.4: Support CERT (co)operation on European level 21
3.1.5 WPK 1.5: Good practice for CERTs to address NIS aspects of cybercrime 23
3.2 WS2 : ENISA as competence centre for securing current & future technologies 24
3.2.1 WPK 2.1: Security & Privacy of Future Internet Technologies 26
3.2.2 WPK 2.2: Interdependencies and Interconnection 28
3.2.3 WPK 2.3: Secure architectures & technologies 30
3.2.4 WPK 2.4: Early warning for NIS 33
3.3 WS3 : ENISA as promoter of privacy & trust 34
3.3.1 WPK 3.1: Identifying and promoting economically efficient approaches to information security 36
3.3.2 WPK 3.2: Deploying privacy & trust in operational environments 37
3.3.3 WPK 3.3: Supporting the review and implementation of the ePrivacy Directive (2002/58/EC) 41

3.3.4 WPK 3.4: European Cyber Security Awareness Month 42
3.4 Summary of Work Streams and Work Packages 45

4. STAKEHOLDER RELATIONS ACTIVITIES 46
4.1 Introduction 46
4.2 Management Board 46
4.3 Permanent Stakeholders Group and NIS Stakeholder networks 47
4.4 National Contact Officers Networks (NCONs) 47
4.5 Stakeholder Relationship Management (SRM) platform 48
4.6 Consultation and follow-up 48
4.7 Summary Table 49

5. PROJECT SUPPORT ACTIVITIES 50
5.1 Promotion and Dissemination activities 50
5.2 Integrating NIS into education 51
5.3 Risk Management activities 51
5.4 Summary of Project Support Activities 52

6. PUBLIC AFFAIRS ACTIVITIES 53
6.1 Public Affairs activities 53
6.1.1 Introduction 53
6.1.2 Aligning to the Policy Environment 53
6.1.3 Public Relations 53
6.1.4 ENISA Digital Communication 53
6.1.5 ENISA Publications and Brand Materials 54
6.1.6 Spokesman and Media Relations 54
6.1.7 ENISA Brand Events 54
6.1.8 ENISA Internal Communication 54
6.2 Summary of Public Affairs Activities 55

7. IT SERVICES 56
7.1 Overview 56
7.2 Summary of Activities related to IT Services 56

8. ADMINISTRATION ACTIVITIES 57
8.1 General Administration 57
8.2 Accounting and Finance 59
8.3 Human Resources 61
8.4 Legal 62
8.5 Summary of Administration Activities 64

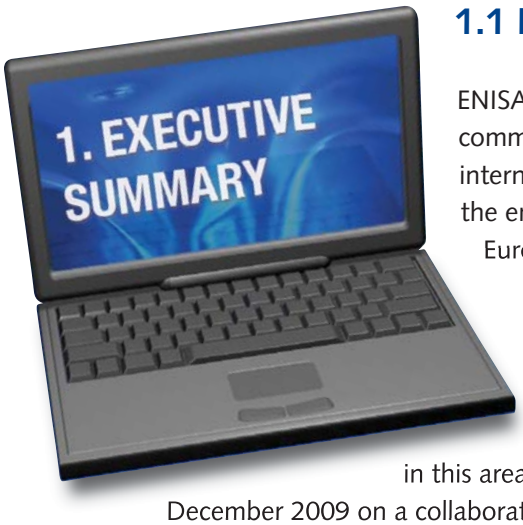
APPENDIX A: OPERATIONAL BUDGET LINES (TITLE 3) 66

APPENDIX B: OPERATIONAL ACTIVITIES 2011 67

ACRONYMS

ABAC:	Accruals Based Accounting (financial management tool)
AD:	Administration Department
ADA:	Administration Department Activity
AR:	Awareness Raising
CAMM:	Cloud Assurance Maturity Model
Cedefop:	Centre for the Development of Vocational Training
CERT:	Computer Emergency Response Team
CIIP:	Critical Information Infrastructure Protection
CSIRT:	Computer Security Incident Response Teams
DG EAC:	DG Education and Culture
DG INFSO:	DG Information Society
DG JUST:	DG Justice
DNS:	Domain Name System
ED:	Executive Director
EDPS:	European Data Protection Supervisor
EFMS:	European Forum for Member States
EFTA:	European Free Trade Association
EISAS:	European Information Sharing and Alert System
ENISA:	European Network and Information Security Agency
EP3R:	European Public Private Partnership for Resilience
ePRIOR:	e-Procurement Application developed by the European Commission
ETF:	European Training Foundation
EuroSCSIE:	European SCADA and Control Systems Information Exchange
FI:	Future Internet
FIA:	Future Internet Assembly
FORTH:	Foundation for Research & Technology
HR:	Human Resources
ICT:	Information and Communication Technologies
ID:	Identity
IoT:	Internet of Things
ISP:	Internet Service Providers
ITSU:	Information Technology Services Unit
MB:	Management Board
MISS:	Missions
MS:	Member States
MTP:	Multi-Annual Thematic Programme

NCO:	National Contact Officer
NCON:	National Contact Officers Network
NIS:	Network and Information Security
NLO:	National Liaison Officer
PA:	Preparatory Actions
PAU:	Public Affairs Unit
PETs:	Privacy Enhancing Technologies
PPP:	Public Private Partnership
PSG:	Permanent Stakeholders Group
Q:	Quarter
RFID:	Radio Frequency Identification
RISEPTIS:	Research & Innovation on Security, Privacy and Trustworthiness in the Information Society
SCADA:	Supervisory Control And Data Acquisition
SLA:	Service Level Agreement
SMART:	Survey and Analysis of EU ICT Security Industry and Market for Products and Services
SME:	Small and Medium Enterprise
SNE:	Seconded National Expert
SR:	Stakeholder Relations
SRM:	Stakeholder Relationship Management
TCD:	Technical Competence Department
WP:	Work programme
WS:	Work Stream



1.1 Background

ENISA has looked at the technology evolution in information and communications technologies (ICT) and the threat situation in internet/cyber space, taking into account a number of factors including the entry into force of the Treaty of Lisbon[1], the Digital Agenda for Europe[2] and expectations of the Member States.

The Commission Communication on Critical Information Infrastructure Protection (CIIP) of March 2009[3] and the conclusions of the Council Presidency of the Tallinn ministerial conference on CIIP[4] have laid the foundations for ENISA's work in this area. In a more general context, the Council Resolution of 18 December 2009 on a collaborative approach to Network and Information Security[5] builds on a number of EU strategies and instruments developed in recent years and provides political direction for how the Member States, the European Commission, ENISA and stakeholders can each play their part in enhancing the level of network security in Europe. The Council Resolution completed a debate on the future of network and information security policy in Europe and the role of ENISA therein.

In parallel, Commission President Barroso announced the policy priorities for the new European Commission, including a major initiative to boost network security as part of the overall Digital Agenda. In early 2010, Mrs. Neelie Kroes was appointed as Vice President of the Commission with the Digital Agenda portfolio. The Digital Agenda is one of the seven flagship initiatives of the Europe 2020 Strategy[6] 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, and attributes an important role to ENISA in relation to the priority area of 'Trust and security'.

Another important development at European scale has been the review of the electronic communications regulatory framework, which resulted, amongst others, in the new provision of articles 13a and 13b in the Framework Directive[7] and in changes in article 4 of the e-Privacy Directive[8].

Finally, the proposal of the Commission for the modernisation of ENISA dated 30 September 2010[9] (COM(2010) 521 final) provides a number of recommendations regarding the role and contribution of ENISA. In particular, this document notes that several of the ongoing developments in NIS policy, notably those announced in the Digital Agenda for Europe, benefit from the support and expertise of ENISA including:

1 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, entered into force on 1 December 2009, 2007/C 306/01.
2 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, Brussels, 19.5.2010, COM(2010)245 final.
3 Commission Communication of March 2009, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149.
4 Ministerial Conference on Critical Information Infrastructure Protection, 27-28 April 2009, Tallinn, Estonia
5 2009/C 321/01
6 EUROPE 2020 – A strategy for smart, sustainable and inclusive growth – COM(2010) 2020.
7 Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)
8 Directive 2002/58 on Privacy and Electronic Communications, (the ePrivacy Directive)
9 Proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA).

- the Commission working with ENISA to draft guidance on promoting NIS standards, good practices and a risk management culture. The first sample of guidance will be produced.
- ENISA organising, in cooperation with the Member States, the 'European month of network and information security for all,' featuring national/European Cyber Security Competitions."

The Work Programme 2011 takes these policy developments at European level into account and moves the Agency one step forward by structuring its work into three separate work streams. Moreover, the current set of Multi-Annual Thematic Programmes (MTPs) will be completed in 2010, whilst the current ENISA mandate ends in March 2012. The work programme therefore foresees a transition phase between the previous objectives and the themes of the future strategy. This transition phase began in 2009 with the introduction of certain preparatory actions in the 2009 Work Programme, notably in the area of Privacy and Trust.

1.2 Structure

1.2.1 Work Streams

The 2011 Work Programme has therefore been structured as three separate work streams, which have been chosen so as to ensure continuity between the former MTPs and the Work Streams (WS) of the future strategy. These work streams are as follows:

- WS1 ENISA as a facilitator for improving cooperation
- WS2 ENISA as a competence centre for securing future technology
- WS3 ENISA as a promoter of privacy, trust and awareness.

1.2.2 WS1 - ENISA as a facilitator for improving cooperation

The principle goal of the first Work Stream is to support the European Commission and the Member States in building on current cooperation schemes to intensify the exchange of information and cooperation between Member States in a number of key areas. This includes providing data and opinions to the Commission in order to assist them policy-making, as well as the identification and promotion of good practice. This work will take into account the work of the European Forum for Member States (EFMS) and the European Public Private Partnership for Resilience (EP3R).

In particular, ENISA intends to:

- Support Member States efforts to deploy article 13a and 13b of the Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive), develop the appropriate incident reporting mechanisms, collect and analyse data and report them back to ENISA.
- Assist Member States and private sector in developing the appropriate capabilities for national and pan European exercises.
- Assist the Commission and Member States in further developing the European Public Private Partnership for Resilience (EP3R).
- Continue to support the CERT community by developing and hosting a collaboration platform for the exchange of information at an operational level and by facilitating cooperation with law enforcement agencies.

1.2.3 WS2 - ENISA as a competence centre for securing current & future technology

The overall objective of the second Work Stream is to assist the Member States and the Commission in identifying and responding to security issues related to current and future technology. This will be achieved by promoting methods and tools for recognising and responding to threats at both the infrastructure and application levels. In this area, ENISA will:

- Address security and privacy risks associated with the Future Internet. As the Future Internet, and the technologies that implement the concept, becomes an integral part of service provisioning and operation of critical infrastructures, any security breaches leading to their unavailability will have effects comparable to an immobilisation of the infrastructure itself.
- Analyse the dependencies of finance and energy sectors on ICT infrastructures from a security and resilience point of view, analyse peering and transit agreements among providers, and assess stakeholder's efforts on mutual aid assistance
- Carry out an analysis of current mechanisms for situation awareness and early warning, assess those mechanisms with regards of timeliness and other factors and derive a proper definition of "early warning". The results will be fed back into the EISAS activities.
- Examine the deployment status of several technologies that have been studied by ENISA during the period 2008 to 2010. In addition, ENISA will support the rollout of some of these technologies.

1.2.4 WS3 - ENISA as a promoter of privacy, trust and awareness

The major objective of the third Work Stream is to promote trust in future information systems by all sections of the population. There are four main activities in this area:

- Understanding and analysing economic incentives and barriers to information security.
- Ensuring that privacy, identity and trust are correctly integrated into new services.
- Supporting the implementation of article 4 of the ePrivacy Directive (2002/58/EC).
- Promoting the establishment of a European month of network and information security for all.

1.2.5 Stakeholder engagement activities

In the area of Stakeholder relations, the following activities are foreseen:

- Management of ENISA's formal bodies (the Management Board and Permanent Stakeholders Group, or PSG)
- Establishment and subsequent management of informal NIS Stakeholder and National Contact Officers (NCO, former NLO) networks;
- Establishment of a platform for managing stakeholder contacts.
- Continued consultation with key stakeholders and follow-up within the project lines.

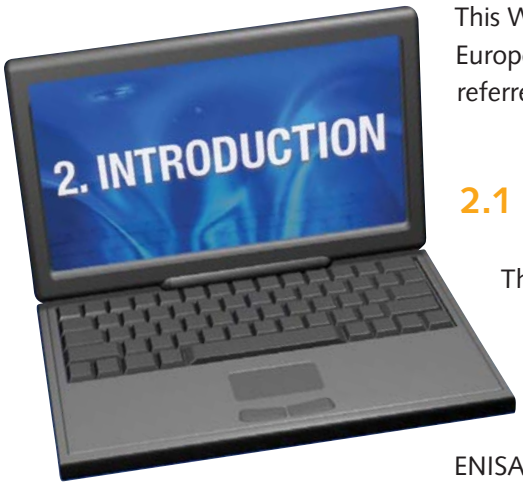
In 2011, the Agency will also continue implementing and further developing a strategic approach, increasing visibility with key actors at political/strategic level and reaching out to NIS communities to promote its work. The Agency's external communication portfolio is complemented by enhancing its internal communication activities. These activities will be carried out within the area of Public Affairs.

1.2.6 Public Affairs activities

In 2011, the Agency will continue increasing visibility with key actors at strategic and decision-making level and reaching out to NIS communities to promote its work and to enable actors to make informed decisions in NIS matters. The Agency's external communication portfolio is complemented by enhancing its internal communication activities.

Remark

This work programme (WP2011) defines the tasks of ENISA in 2011. It has no correlation to the Agency's internal organisational structure.



This Work Programme defines and describes the activities of the European Network and Information Security Agency (hereafter also referred to as the Agency) foreseen for 2011.

2.1 Relation to the previous work programme

The Multi Annual Programmes (MTPs) defined for the previous 3 year period end in December 2010. In 2010, ENISA launched two new Preparatory Actions (PAs) in the areas of 'Identity, Privacy & Trust' and 'Economics of NIS'.

ENISA will use 2011 as a transition year to follow up key work packages of the old MTPs and PAs. This is in line with the current demands of the Commission's communication, the Council's directives and Member States' needs. ENISA's aim is to target their deliverables more closely to the stakeholder's needs and prepare for the new mandate after March 2012. This has resulted in the definition of the following key topics, hereafter referred to as Work Streams (WS):

- WS1 ENISA as a facilitator for improving cooperation
- WS2 ENISA as a competence centre for securing future technology
- WS3 ENISA as a promoter of privacy & trust.

2.2 Policy context

2.2.1 Background

This Work Programme has been developed against the background of a rapidly changing policy context and continued rapid evolution of information security-related threats. It has taken account of various changes at EU level, such as the new Treaty of Lisbon, the EU regulatory framework for electronic communications, the Digital Agenda for Europe, the Council Resolution of Dec 2009 , the CIIP Action Plan and the Granada Non-Paper. All these policy statements effectively call upon ENISA to support the Commission and the Member States by providing expertise in the area of Network and Information Security.

2.2.2 The CIIP Action Plan

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. This action plan received a high level of support from the Member States. The Presidency conclusions of the Tallinn Ministerial Conference on CIIP state that "there is an urgent need for Member States and all stakeholders [including ENISA] to commit themselves to swift action in order to enhance the level of preparedness, security and resilience of CIIs throughout the European Union". It also states that "the Communication by the European Commission on CIIP furnishes a solid basis for taking such urgent action as is necessary".

2.2.3 The Electronic Communications Regulatory Framework

Another major initiative relevant to network security is the recently adopted 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. These provisions aim at strengthening obligations for operators to ensure security and integrity of their networks and services, and to notify breaches of security, integrity and personal data to competent national authorities and assign to ENISA specific tasks.

2.2.4 The Council Resolution

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 Resolution should also be considered as the culmination of the public debate on the direction of network and information security in Europe and the role of ENISA therein.

2.2.5 The Digital Agenda

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.

In the area of trust and security, the Digital Agenda foresees a number of initiatives including the cooperation of relevant actors to be organised at global level to fight security threats. Moreover, internationally coordinated information security targeted actions should be pursued and joint action taken. It foresees a reinforced and high level NIS policy, including legislative initiatives, such as a modernised ENISA and measures allowing faster reactions in the event of cyber attacks, including a CERT for the EU institutions.

Among others the Digital Agenda highlights the following areas of activity where ENISA could help to:

- Support the Commission to develop a strategy on identity management, including the review of the eSignature directive and promotion of mutual recognition of eID processes across the EU.
- Enhance global cooperation between players, including support for a strong global Risk Management.
- Support the review of EU data protection framework and the extension of security breach notification provisions
- Support operational forces on Member State and European level to successfully combat cyber attacks, including the support for establishing and reinforcing national / governmental CERTs in all MS and enhance CERT cooperation on European level
- Enhance the preparedness of Europe to combat cyber attacks by supporting the Member States to carry out large scale attack simulations and supporting EU-wide cyber security preparedness exercises
- Securing future technologies by support the implementation of ICT standards in Europe and, in particular, support a EU-wide strategy on cloud computing

- Foster the establishment of a proactive networking community by support the Member States in establishing reporting points for illegal content and run respective awareness campaigns and by helping Member States to effectively inform and alert their citizens and SMEs about NIS related issues

2.2.6 The Commission proposal on the future of ENISA

This 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 ongoing developments in NIS policy (notably those announced in the Digital Agenda for Europe) that would benefit from the support and expertise of ENISA. These include:

- Strengthening NIS policy cooperation by intensifying activities in the European Forum of Member States (EFMS),
- Strengthening cooperation and partnering between the public and the private sector, by supporting the European Public-Private Partnership for Resilience (EP3R).
- Putting the security requirements of the regulatory package on electronic communications into practice, for which ENISA's expertise and assistance is required.
- Facilitating EU-wide cyber security preparedness exercises with the support of the Commission.
- Establishing a CERT (Computer Emergency Response Team) for the EU institutions.
- Mobilising and supporting the Member States in completing and where necessary in setting up national/governmental CERTs.
- Raising awareness of NIS challenges.

The work streams W1, W2 and W3 that are described in this document have been developed in this context and they support this overall political agenda.

2.3 Key challenges

In order to optimally support the policy initiatives outlines in the last section, ENISA is faced with a number of important challenges. The most important challenges are as follows:

2.3.1 Fostering a proactive NIS community

Achieving a coherent response to the evolving NIS threat landscape, in which all actors contribute to define and implement a global approach to securing infrastructure and reacting to incidents, remains the number one challenge in modern information security. Whilst Member States can reasonably expect to master natural disasters and malicious attacks that take place within their own borders, incidents that have a global impact will require a coordinated prevention strategies and response based on strong collaboration. This will only be possible if the community at large is both aware of the role that it has to play and has the necessary competence to carry out the associated activities.

2.3.2 Assisting Member States in implementing secure services

Secure infrastructure is a necessary condition for supporting the economy of the future, but it is not in itself sufficient. The future economy will be increasingly based on global electronic services and, given that we cannot predict how the global networked environment will evolve, it is to be expected that such services will be designed to be able to operate under a number of different conditions. In particular, services should not depend exclusively on the underlying network and infrastructure for their security, but in many cases should be able to operate over an insecure network.

ENISA will support this move towards secure services by promoting a holistic approach to security that covers the applications, the infrastructure upon which they run and the process environment that they are designed to support.

2.3.3 Promoting uptake of ICT by the citizen through an enhanced framework for privacy and trust

Technological advances are likely to be one of the main stimuli for economic growth in the coming years, but in order to leverage the advantages that such advances bring it will be necessary to ensure that citizens are prepared to adopt new technology. Currently, security and privacy concerns are limiting the extent to which the European citizen is adopting new technology.

By assisting the Commission and Member States in creating a framework that will allow citizens to make use modern technologies in a secure manner whilst still retaining control over privacy issues, ENISA hopes to contribute to the establishment of a performant European economy.

2.4 ENISA's role

ENISA is in a unique position to provide advice and assistance falling within the Agency's scope to Member States, the European Parliament and the European Commission. The underlying purpose of ENISA's role in responding to requests as foreseen by the ENISA Regulation lies in the increase of the levels of network and information security.

The capacity to provide prompt, independent and high quality response to requests received from the Commission, Parliament and Member States' competent bodies gives the Agency a bridging role between EU and national institutions.

The Agency supports an open multi-stakeholder dialogue and, for that reason, maintains close relations with industry, the academic sector and users. It also sets and develops contacts with a network of national representatives of competent bodies and with major individual experts through ad-hoc Working Groups. Less formal, but equally efficient interactions are in progress through virtual expert groups and platforms to gather and disseminate expert recommendations and to facilitate information exchange with and between public and private sector parties. Moreover, the Agency maintains relations with EU Bodies and international organisations in the field of NIS.

3.1 WS1 : ENISA as facilitator for improving cooperation

WS NAME :

WS1: ENISA as facilitator for improving cooperation

DESCRIPTION OF THE PROBLEM TO SOLVE :

The principle goal of the first Work Stream is to support the European Commission and the Member States in building on current cooperation schemes to intensify the exchange of information and cooperation between Member States in a number of key areas. This includes providing data and opinions to the Commission in order to assist them in drafting new regulation as well as the identification and promotion of good practice in support of such legislation. This work will feed into and take into account the discussions at the European Forum for Member States (EFMS) and the European Public Private Partnership for Resilience (EP3R).

The problems to be solved have been described in other documents, notably the European Commission's Communications on Security (COM 2006 251), the CIIP (COM 2009 149), which highlighted the importance of network and information security and resilience for the creation of a single European Information Space, and the Digital Agenda. More generally, availability, integrity and continuity of public communication networks are of major importance in a converging environment of fixed and mobile infrastructures. A totally interconnected and networked environment promises significant opportunities but also creates additional security risks. As interdependencies become complex, a disruption in one infrastructure can easily propagate across boundaries (geographical and jurisdictional) as well as into other infrastructures and have a European-wide impact.

The global nature of telecommunication business requires a common approach to deal with issues such as resilience and security of public communication networks. Several Member States have already developed, or are in the process of developing, strategies, policies and regulatory initiatives to cope with these issues. These strategies propose a number of actions aiming at developing an integrated EU approach to enhance the security and resilience of critical communication networks by complementing and adding value to national programmes as well as to other bilateral and multilateral cooperation schemes between Member States. Most of these strategies are based on co-operation with providers, sharing of information on incidents and threats, development of good practices, development of preparedness measures and testing of them through exercises.

Despite these efforts, the situation across Europe as regards the obligations and requirements to ensure and enhance the security and resilience of such networks is highly fragmented. The smooth functioning of the Internal Market and the demand of global players call for common requirements, rules and practices across the EU.

In carrying out the activities associated with this workstream, ENISA will support and contribute to initiatives launched by the Commission in order to enhance the security and resilience of critical communication information infrastructures, such as the European PPP on Resilience (EP3R) and the pan European Forum of Member States (EFMS).

DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

In 2011 ENISA intends to:

- Support Member States, the Commission and private sector in their efforts directed to the implementation of articles 13a and 13b of the EU regulatory framework for electronic communications.
- Support Member States in enhancing their capabilities on national and carrying out pan-European Exercises
- Continue to reinforce CERTs in the Member States
- Continue to support CERT (co)operation on European level

WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

This Work Stream supports the following high-level goals:
Facilitating information exchange amongst Member States on topics related to resilience, CIIP and response communities.
The implementation of the CIIP Action Plan as detailed in COM(2009)149.
Meeting the obligations stemming from Article 13a of the EU regulatory framework for electronic communications.
Support the cooperation of CERT community on a EU level.

STAKEHOLDERS + BENEFICIARIES

National Regulatory Authorities
NIS competent bodies
Member States Governments and EU Policy and Decision Makers
National / governmental CERTs
Public Communications Networks and Services Providers (fixed, mobile and IP-based) Internet Service Providers (ISPs)
Associations of Providers (ETNO, ECTA, EUROISPA, EICTA, EuroIXs, ETIS)
Internet Exchange (IXPs)
Suppliers of Network Components, Systems and Software

WHY ENISA?

Major disruptions involving the network infrastructure and information systems of several Member States can only be effectively dealt with on a multilateral basis. They require integration of legislation, planning, organizations, infrastructure, and technical efforts. By its designation, ENISA is well-positioned to promote and facilitate European Union joint policies, activities, and procedures in this area.

3.1.1 WPK 1.1: Supporting Member States in implementing article 13a

WS Name
WS1: ENISA as facilitator for improving cooperation

WORK PACKAGE NAME:
WPK 1.1: Supporting Member States in implementing article 13a

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):	
SMART goal: By end of Q4 2011, at least 18 Member States take part in ENISA efforts to support harmonised implementation of article 13 a	**KPI:** # of Member States
SMART goal: By end of Q4 2011, at least 10 providers take part in ENISA efforts to support harmonised implementation of article 13 a	**KPI:** # of providers
SMART goal: By end of Q4 2011, at least 15 Member States adopt the proposed annual incident reporting scheme to ENISA	**KPI:** # of Member States

DESCRIPTION OF TASKS:

Article 13a of the new Framework Directive calls on Member States to ensure that providers take appropriate measures to manage the risks posed to the security of their networks and services and to notify the competent national regulatory authority of a breach of security that has had a significant impact on the operation of networks and services.

Article 13a also specifies that the Commission may adopt appropriate technical implementing measures taking ENISA's utmost technical opinion under consideration. Member States shall adopt and publish by 25 May 2011 the laws, regulations and administrative provisions necessary to comply with the revised directives.

The revised framework refers to the supporting role of ENISA in enhancing the level of security of electronic communications by providing expertise and advice, promoting the exchange of good practices and contributing to the harmonisation of appropriate measures across Europe.

ENISA, together with the Member States, has already developed knowledge and expertise on several issues related to article 13a. In 2009, this work resulted in the publication of a good practice guide on national incident reporting and good practices on providers' measures. ENISA has also analysed the area of security and resilience metrics and developed a new taxonomy which covers corporate, sectoral, national and Pan-European levels.

In 2010 ENISA, acting as a facilitator, identified the appropriate competent regulatory authorities and engaged them in a structured dialogue on relevant issues, e.g. incident reporting (e.g. conditions, parameters, impact), minimum security and resilience requirements, reporting annual incident reports to ENISA.

In 2011 ENISA will continue supporting Member States in their efforts to implement article 13a in a harmonised way. The Agency will follow up the transposition process in each MSs, provide expertise and knowledge to competent authorities of MS, and facilitate the information sharing among them on implementation issues. This would be done through dedicated conferences on issues of common interest proposed by the Commission, but also mailing lists and a dedicated online forum.

ENISA will assist the Commission in preparing guidelines and good practices to support Member States in implementing paragraph 1 and 2 of article 13 a. The guidelines and good practices will help Member States to take the "appropriate technical and organisational measures" that would ensure that providers' networks and services are secure and resilient. ENISA will work with all stakeholders to take stock of the relevant good practices and technical standards leveraging also the activities of EP3R. In addition, ENISA will provide technical assistance to the Commission for the adoption of the technical implementing measures with a view to harmonising the measures referred to in paragraph 1, 2 and 3 of article 13 a.

ENISA will also engage Member States, Competent Authorities and the private sector in a dialogue on annual reporting of incidents to ENISA. Through this dialogue ENISA aims to develop a trusted framework for collecting and analysing incidents. Possible issues to be considered are the nature and level of abstraction of the information collected, the use and purpose of the information, the expected added value, a definition of the template, the framework and the procedures for reporting to ENISA aggregated reports on incidents, etc. Through this activity ENISA will aim at developing a comprehensive information sharing, data collection and analysis framework supported by the usage of well defined and agreed metrics and indicators.

OUTCOMES AND DEADLINES:

Reporting Incidents to the Commission and ENISA – Framework Q4 2011 (report)
Minimum Security Levels – Guidelines and Good Practices – Q4 2011 (report)

STAKEHOLDERS

National Regulatory Authorities
Authorities dealing with the resilience of public communication networks and services
Telecommunications Providers (fixed, mobile and IP-based)
Internet Service Providers (ISPs)
Sector Associations

RESOURCES FOR 2011 (person months and budget)

- 19,5 person months
- 150 kEuro

LEGAL BASE

- ENISA regulation article 3
- EC CIIP communication COM(2009) 149 (chapter 5.1, 5.2, 5.3)
- Digital Agenda (chapter 2.3)
- Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

3.1.2 WPK 1.2 : Preparing the Next Pan-European Exercise

WS Name

WS1: ENISA as facilitator for improving cooperation

WORK PACKAGE NAME :

WPK 1.2: Preparing the Next Pan-European Exercise

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: By end of Q4 2011, at least 12 Member States take part in the development of the roadmap and the future scenarios	**KPI:** # of Member States
SMART goal: By end of Q4 2011, at least 12 Member States take part in ENISA efforts towards the second pan European exercise	**KPI:** # of Member States
SMART goal: By end of Q4 2011, at least 5 Member States organise seminars and prepare plans for national exercises	**KPI:** # of Member States

DESCRIPTION OF TASKS:

Pan- European exercises on large scale network security incidents were put forward in the CIIP Action Plan[10]. The initiative was endorsed within the Presidency Conclusions[11] of the Tallinn Ministerial Conference and in the Council Resolution 2009/C 321/01[12] adopted in December 2009. In all three main policy documents ENISA was called upon to co-ordinate, facilitate, organise and manage the first pan-European exercises by end of 2010.

The first pan-European exercise was a table-top exercise, involved only government authorities. The main objective was to build trust among Member States. It aimed at increasing the understanding on how cyber incidents are handled nationally and how cross-border cooperation could be enhanced. At the time of writing, all Member States participate in the first pan European exercise either as observers or as participants.

Recognising the importance of the topic for Europe's information infrastructures and services, ENISA will engage all relevant stakeholders in a dialogue on the future of pan European exercises in coordination with EFMS and possibly leveraging EP3R as a platform. Through structured dialogue with relevant stakeholders the Agency will develop a common vision, a roadmap for future actions and a portfolio of possible scenarios for future exercises of varying complexity. The results of this action will help ENISA to focus its efforts towards the second pan European exercise. More specifically the Agency will agree an approach for engaging relevant stakeholders with the Member States, prepare the planning of the second exercise, and launch the first discussions on the possible scenario of the second exercise.

10 COM(2009)149 in March 2009

11 See http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

12 See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF

Following the successful completion of the first exercise, ENISA will continue enhancing its knowledge, expertise and capabilities in this area. The Agency will follow the EuroCybex project as a technical advisor, in EuroCybex project[13].

ENISA will also ask the Member States to consider the possibilities of establishing co-operation with other cross-country and/or international exercises. This dialogue will help ENISA to further enhance its knowledge and expertise on organisational and managerial aspects of complex, pan European exercises. This knowledge will complement and enrich the existing Framework for running complex pan European exercises.

ENISA will continue to support Member States in organising and running national exercises and will therefore continue to evolve and promote the Good Practice Guide on National Exercises. Through targeted seminars and dedicated workshops ENISA will try to build up the expertise and knowledge of the appropriate national stakeholders.

Finally, ENISA will take stock of national resilience contingency plans, identify commonalities and differences among them, assess and analyse them, engage private and public experts in a structured dialogue (e.g. workshops and online means) on good contingency measures, assess means to test them regularly, and finally develop recommendations and good practices on good and well functioning national contingency plans. ENISA will use all possible means to engage private and public stakeholders including EP3R.

OUTCOMES AND DEADLINES:

Roadmap and Scenarios for future exercise – Q4 2011 (report)
Status of Second Pan European Exercise - Q4 2011 (report)
Seminars with MS on national exercises – Q1-Q4 2011 (workshops)
Good Practice Guide on National Contingency Plans – Q4 2011 (report)

STAKEHOLDERS

Organisations in Member States dealing with exercises (e.g. national regulatory authorities/competent bodies, ministries, national/gov CERTs, dedicated agencies)
Telecommunications providers (fixed, mobile and IP-based)
Internet Service Providers (ISPs)

RESOURCES FOR 2011 (person months and budget)

- 21,5 person months
- 140 kEuro

LEGAL BASE

ENISA regulation article 3
EC CIIP communication COM(2009) 149 (chapter 5.1, 5.3)
Council Resolution 2009/C 321/01 (article VIII)
Digital Agenda (chapter 2.3)

[13] This is an EPCIP sponsored project that aims to deliver a pan European exercise in 2011

3.1.3 WPK 1.3: Reinforcing CERTs in the Member States

WS Name

WS1: ENISA as a facilitator for improving cooperation

WORK PACKAGE NAME :

WPK 1.3: Reinforcing CERTs in the Member States

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: By Q4 2011, 80% of updates in CERT inventory are confirmed	**KPI:** % confirmed updates
SMART goal: By Q4 2011 at least two TRANSITS trainings have been organised with support by ENISA	**KPI:** # of trainings supported

DESCRIPTION OF THE WORK PACKAGE

ENISA has developed and will continue to develop tools (such as CSIRT setting-up and running guides, cooperation guide and CSIRT exercise collection) for strengthening the CERT community and their co-operation and focuses on helping to set-up new national / governmental CERTs in the Member States.

To this end the support of the very successful TRANSITS trainings for CSIRT staff members taking place at least twice a year in Europe will be continued[14]. Member States' requests for special CERT staff trainings may be accommodated, as it has been done in the past, to close the gaps of CERT services in Europe, especially in national / governmental CERT coverage and baseline capabilities. (The ENISA CERT Inventory will be updated to reflect the developments in the European landscape accordingly).

In addition, in 2011 ENISA will look for ways to improve communication with the CERTs and other stakeholders (institutions in the Member States, European Commission, etc.), especially when it comes to sharing information in a secure way. "Secure" in this respect means transportation of information, assuring confidentiality, integrity and authenticity of the data.

We will take stock of existing solutions, developments and research in that area, and will by the end of 2011 produce an analysis of the requirements and offer guidance on a suitable channel to start with (without anticipating the results of the stock taking a first approach could be a secure web portal and an encrypted mailing list), including a roadmap for implementation and future development.
The result of this work will feed into the ongoing dialogue with the key stakeholders on the further deployment of the "Baseline capabilities for national / governmental CERTs".

[14] Provided that the organiser of the previous regular TRANSITS courses continue this effort.

OUTCOMES AND DEADLINES:

Updated "ENISA Inventory of CERTs in Europe" in Q2 and Q4
At least 2 TRANSITS courses supported by Q4
Proposal for secure communication channel(s) and roadmap by Q4

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Design and implementation: ENISA; Users: CERT community, Member States institutions, European Commission, etc.

RESOURCES FOR 2011 (person months and budget)

- 10 person months
- 26 kEuro

LEGAL BASE

ENISA regulation article 3
EC CIIP communication COM(2009) 149 (chapter 5.1, 5.2, 5.3)
Council Resolution 2009/C 321/01 (article VI.3 and VIII)
Digital Agenda (chapter 2.3)

3.1.4 WPK 1.4: Support CERT (co)operation on European level

WS Name

WS1: ENISA as facilitator for improving cooperation

WORK PACKAGE NAME :

WPK 1.4: Support CERT (co)operation on European level

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: By Q4 2011, at least 10 references to each report from external websites, official publications, discussions on mailing lists or other means.

KPI: # of references
KPI: # of download

DESCRIPTION OF THE WORK PACKAGE

This work package is intended to support the operation and cooperation of CERTs at a European level. The main activity of this package is to explore ways to deals with barriers and incentives of cross border collaboration, especially when it comes to legal obstacles for cross-border information sharing (data protection and other issues).

This package also intends to analyse how, on a European level, CERT cooperation can be further facilitated, by examining operational needs and (if existing) overlaps. Last but not least this work package will include a continuation of provision of services for Member States and European institutions with regards to the setting-up and operation of CERTs, training and exercises, and the reflection of our work in form of an updated CERT inventory.

1) Barriers and incentives for cross-border collaboration and information sharing – a follow-up report and good-practice guide, going into more detail what prevents and assists collaboration cross-border, for national / governmental CERTs and other stakeholders. The work will, for example, take into account the "Legal Handbook for CSIRTs" and other information such as that arising out of Commission funded projects.
2) Analysis "operational gaps and overlaps on European level" a report on how cross-border collaboration (of CERTs and other stakeholders) can be reinforced (with regards to incident response coordination and other issues). One aspect of this work will be the support for CERTs in preparing their contribution to the pan-European exercises in 2012.

The result of this work will feed into the ongoing dialogue with the key stakeholders on the further deployment of the "Baseline capabilities for national / governmental CERTs".

OUTCOMES AND DEADLINES:

Draft report on barriers of cross-border information sharing of CERTs, and how to address them.
An overview (in form of a report) of operational gaps and overlaps and how to address them on European level.

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

CERT community
Member States institutions
European Institutions

RESOURCES FOR 2011 (person months and budget)

- 21 person months
- 160 kEuro

LEGAL BASE

ENISA regulation article 3
EC CIIP communication COM(2009) 149 (chapter 5.1, 5.2, 5.3)
Council Resolution 2009/C 321/01 (article VI.3 and VIII)
Digital Agenda (chapter 2.3)

3.1.5 WPK 1.5: Good practice for CERTs to address NIS aspects of cybercrime

WS Name

WS1: ENISA as facilitator for improving cooperation

WORK PACKAGE NAME :

WPK 1.5: Good practice for CERTs to address NIS aspects of cybercrime

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: By Q4 2011, at least 10 references to each report from external websites, official publications, discussions on mailing lists or other means.	**KPI:** # of references
SMART goal: At least 50% of the EU population is represented at the workshops	**KPI:** % of EU population represented
SMART goal: Workshop participants score at least as 3 on a scale of 1-5	**KPI:** Average feedback on scale of 1-5 per workshop

DESCRIPTION OF THE WORK PACKAGE

This activity aims at improving the capability of CERTs to address NIS aspects of cybercrime. It aims at supporting National / Governmental CERTs and their hosting organisations and Member States. Activities will mainly be derived from gap analyses and input from the stakeholders. The activities comprising this work package are (a) production of a good practice guide for CERTs in addressing NIS aspects of cybercrime and (b) the sixth ENISA workshop for CERTs in Europe.

First draft "Good practice for CERTs in addressing NIS aspects of cybercrime": This will be a first collection of good practices developed by mature CERTs, including among other things roles & responsibilities, workflows and cooperation with other key players such as law enforcement. Both communities (CERTs and law enforcement) work, mainly on their own, in different areas of NIS. The activity in this WPK shall, in a first round, shed a light on commonalities and differences between these two, with the main goal to better understand obstacles in cooperation and how to circumvent them.

Sixth ENISA Workshop CERTs in Europe: ENISA will seek the dialogue with the stakeholders by offering a workshop for key players in the Member States and the European Commission. The sixth edition of the workshop "CERTs in Europe" will again focus on a current topic relevant for National / Governmental CERTs. Tentative topic: good practice for CERTs to address NIS aspects of cybercrime.

OUTCOMES AND DEADLINES:

First version of a good practice collection (report)
6th ENISA workshop CERTs in Europe

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

CERT community, Member States institutions, research institutions, etc.

RESOURCES FOR 2011 (person months and budget)

- 16,5 person months
- 120 kEuro

LEGAL BASE

ENISA regulation article 3
EC CIIP communication COM(2009) 149 (chapter 5.1, 5.2, 5.3)
Council Resolution 2009/C 321/01 (article VI.3 and VIII)
Digital Agenda (chapter 2.3)

3.2 WS2 : ENISA as competence centre for securing current & future technologies

WS NAME :

WS2: ENISA as competence centre for securing current & future technologies

DESCRIPTION OF THE PROBLEM TO SOLVE :

The overall objective of the second Work Stream is to assist the Member States and the Commission in identifying and responding to security issues related to current and future technology. This will be achieved by promoting methods and tools and standards for recognising and responding to threats, vulnerabilities and risks at both the infrastructure and application levels.

Correctly securing information systems and services in the future will require recognising and reacting to a number of key trends. These trends are already identifiable in the current environment and are largely driven by changes in technology. Our inability to handle such rapid changes in technology is highlighted by the increasing number of criminal attacks on the data of companies, government entities and private users – and is frequently the subject of media attention.

Recently, cases in which the privacy of data was violated have attracted much attention and illustrates the fact that the way in which data is handled within companies is often problematic. Although this is often due to a lack of personnel and financial resources, there are more fundamental problems to be solved. Truly effective solutions to securing systems take account of the technological complexity of the implementation and are implemented in a way that allows for scalability and offer reasonable flexibility.

In addition, modern technologies are often based on ideas that are not aligned with traditional security solutions, which makes secure implementation even more difficult. Highly distributed architectures for instance aim to render the location of objects and data irrelevant (which makes securing such data much difficult) and applications are tending to give more power to the end user. Even the most innovative technological security measures can only provide limited protection if employees or external suppliers can access data and misuse them. As an example of these trends, security experts also have to worry about the careless handling of data in the interactive Web 2.0 applications, particularly, on the increasingly popular social network sites. Without hesitation, users provide detailed personal information in their profiles; often forgetting that information on the Internet is, and will remain, accessible to practically anyone.

DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

This Work stream covers the following areas:

- Security and privacy of Future Internet technologies, in particular those associated with the cloud.
- Securing interdependencies and interconnection
- Secure architectures and technologies
- Early warning for NIS (EISAS)

In the first of these areas, ENISA will look at both security and privacy aspects of technologies that will support the Future Internet. Areas of particular interest are the Internet of Things (IoT), Cloud Computing and mobile computing (smart phones). The approach taken will be as follows:

- To identify and support the development of reliable sources of data about the nature, distribution and severity of current security incidents and risks (threats and vulnerabilities).
- Based on priorities derived from the information collected,, to identify, support and where necessary initiate fora, methodologies, reference architectures, secure development programmes, educational programmes and principles focused on addressing the identified risks.
- To identify and support the development of reliable assurance mechanisms for security infrastructure and applications by collaborating with industry experts.

In the area of interdependencies and interconnection ENISA will take stock and analyse the specific requirements of two critical sectors on information and communication networks, namely finance and energy sectors. Leveraging EP3R as means to identify and engage relevant stakeholders in the study, ENISA will holistically assess technical issues (e.g. logical, physical, application layers, replication and diversity of services and data, data centres), peering and transit issues (e.g. SLAs), market, policy and regulatory issues. The result will be recommendations for targeted stakeholders but also guidelines and good practices for enhancing the security and resilience of these inter-depended networks.
Under the heading 'Secure Architectures and Technologies' ENISA will examine the deployment status of several technologies that are strongly associated with improved resilience and that have been studied by the Agency during the period 2008 to 2010. In addition, ENISA will support the rollout of some of these technologies.

Finally, ENISA will look at the concept of "early warning" and situational awareness in the Internet. The activity is two-fold: the first part aims at enhancing the capability of CERTs to keep them informed, the second part involves timely information sharing and alerting of constituents of CERTs, with an emphasis on citizens and SMEs.

WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

Facilitate the exchange of knowledge among Member States and provide updated information
Give advice on technical issues related to security to the Member States and the European Commission
Act as a central point of reference for security issues in this field.

STAKEHOLDERS + BENEFICIARIES

European Commission
Member States
Industry
Academia

WHY ENISA?

The problems addressed in this work stream transcend national boundaries. It is therefore necessary to analyse and respond to these issues at a European level, complementing the work that is being carried out in individual Member States. Because of its expertise and neutrality, ENISA is well-positioned to give advice to the European Commission and the Member States on the pan-European aspects of securing current and future technologies. The topic of this program fits well within the scope of ENISA's tasks.

3.2.1 WPK 2.1: Security & Privacy of Future Internet Technologies

WS Name

WS2: ENISA as competence centre for securing current & future technologies

WORK PACKAGE NAME :

WPK 2.1: Security & privacy of Future Internet technologies

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: Number of contributions made in the deliverables of the IOT EG	**KPI:** # Contributions
SMART goal: At least 5 citations of smartphone paper in reputable journals.	**KPI:** # Citations

DESCRIPTION OF TASKS:

In tackling the issue of security and privacy for the Future Internet, this work package focuses on three different areas involving separate technologies that are elements of the Future Internet vision.

Security and privacy in the 'Internet of Things': In its Communication of June 2009 entitled 'Internet of Things — An action plan for Europe'[15] the European Commission presented the vision of an Internet of objects that communicate and exchange large amount of data between them. In this Communication the European Commission identified a number of 'Lines of action' for the EU. Among them two areas of particular interest are:

- Defining a set of principles underlying the governance of IoT (Line of Action 1), and
- Providing a policy framework that enables IoT to meet the challenges related to trust, acceptance and security (Line of action 4).

Considering the above and the work already performed by ENISA in the field of identifying emerging and future risks of IoT/RFID, including the support brought in 2010 to the European Commission, the Article 29 Data Protection Working Party, and the industry on the RFID Privacy Impact Assessment Framework, ENISA will assist the EC in identifying appropriate policy options towards developing a policy framework from IoT in the framework of the Digital Agenda for Europe, always from the point of view of information security and privacy. Furthermore, ENISA will contribute to the discussions of information security and privacy requirements that could then be used by stakeholders as input in an IoT governance model.

In view of the above, ENISA will participate in the Expert Group on the Internet of Things (Commission Decision 2010/C 217/08) where ENISA will concentrate on the security and privacy considerations.

Cloud computing and IT service procurement: security requirements for EU government bodies: Cloud computing is an emerging use of internet technologies which is seen as a strategic imperative by many European government bodies. ENISA has already received requests for help from government agencies in Europe requiring objective security advice in implementing and procuring cloud computing projects. Such requirements are only going to increase in the coming years.

Furthermore, cloud providers, with globally distributed cloud data centres, are gradually becoming so large that the failure of a single provider may have implications for a whole national economy. In this sense, ENISA considers it important to cover not only critical infrastructures but also "critical service delivery platforms". This is in line with the Digital Agenda, which proposes an EU-wide strategy on 'cloud computing' (notably for government and science).

In 2011, our previous work in this area will be followed up with an initiative which pilots the CAMM (Cloud Assurance Maturity Model) cloud assurance criteria in government procurement processes. Furthermore, ENISA will investigate the use of these and additional criteria in the audit and monitoring of existing government cloud contracts through consultation with stakeholders and brokerage of pilot projects. This approach promises significant efficiency savings not only by enabling the use of cloud computing but also by eliminating duplication in procurement procedures and assurance processes.

Smartphones: secure deployment and development guidelines for governments and business: Smartphones have already realised many aspects of the vision for the Future Internet. The smartphone includes a powerful set of sensors, a user interface and network connectivity incorporated in a device which is in most cases within 1m of its owner 24 hours a day. Smartphones are expected to play an increasingly important role in the realisation of the Future Internet for governments, businesses and consumers.

15 http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

ENISA will follow-up on the 2010 work on smartphone application security, as well as the stocktaking work done on secure software engineering. We will follow up on the risk analysis and recommendations arising from the 2010 smartphone report. Target areas include implementations within government organisations, guidelines for applications developers and secure and privacy respecting software engineering programmes, as well as EU research and safer internet programmes. One example area is to address the lack of privacy guidelines available to application developers. This will also give ENISA the opportunity to explore ways of contributing to the wider field of secure software engineering best practice.

OUTCOMES AND DEADLINES:

Participation and contribution to work program of the High-Level IoT expert group.
Conference on cloud assurance in Q2 2011
Pilot study of cloud computing guidelines by Q4 2011
Guidelines on an area of smart phone application security and privacy Q4 2011

STAKEHOLDERS

Member states, Industry

RESOURCES FOR 2010 (person months and budget)

- 31,5 person months
- 80 kEuro

WORK PACKAGE PROPOSED BY

Information Society and Media directorate General

LEGAL BASE

ENISA regulation article 7.
Communication on the Internet of Things COM(2009)278
COMMISSION DECISION of 10 August 2010 setting up the Expert Group on the Internet of Things (2010/C 217/08)

3.2.2 WPK 2.2: Interdependencies and Interconnection

WS Name

WS2: ENISA as competence centre for securing current & future technologies

WORK PACKAGE NAME :

WPK 2.2: Interdependencies and interconnection

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: By end of Q4 2011, at least 10 financial companies and 10 energy providers take part in the study on inter-dependent networks	**KPI:** # financial companies # energy providers
SMART goal: By end of Q4 2011, at least 10 providers and IXPs contribute to the study on interconnected networks	**KPI:** # providers and IXPs
SMART goal: By end of Q4 2011, at least 10 providers and 5 Member States contribute to the study on mutual aid assistance	**KPI:** # providers # Member States

DESCRIPTION OF TASKS:

ICT infrastructures provide critical support for many sectors, including notably critical sectors such as energy, finance and transport. These different sectors have varying needs and requirements for the resilience and security of the services offered to them by ICT infrastructures. The interdependencies on interconnected networks and services introduce systemic risks and threats that need to be further analysed and studied at the interfaces level. The CIIP Action Plan[16] highlighted the importance of interdependencies and interconnection.

In previous studies ENISA worked with Member States and the private sector to analyse the resilience and security aspects of core ICT networks. However the inherent interdependencies among networks, applications, and services across sectors were not thoroughly studied.

In this work package ENISA will take stock and analyse the specific requirements of two critical sectors on information and communication networks, namely the finance and energy sectors. Using EP3R as means to identify and engage relevant stakeholders in the study, ENISA will assess technical issues (e.g. logical, physical, application layers, replication and diversity of services and data, data centres), peering and transit issues (e.g. SLAs), market, policy and regulatory issues. The result will be recommendations for targeted stakeholders but also guidelines and good practices for enhancing the security and resilience of these inter-depended and inter-connected networks.

ENISA will also analyse the increasing reliance of SCADA systems on internet and the advent of smart grids. Using EP3R as a platform for identifying and engaging relevant stakeholders in the study, ENISA will first identify all relevant national, pan European (e.g. EuroSCSIE) and international initiatives and then try to engage them in a structural dialogue on the risks and threats of such interdependencies. The Agency will then analyse the situation and develop recommendations for targeted stakeholders. These recommendations will help stakeholders to improve the security, safety and resilience of their SCADA systems.

Finally, ENISA will analyse stakeholder's efforts on mutual aid assistance and co-ordinated response and recovery approaches. The main aim is to develop and propose good practice guides for establishing such mechanisms at ecosystem/sector level.

16 COM(2009)149 in March 2009

OUTCOMES AND DEADLINES:

Interdependencies of Energy, Finance and Transport Sector on ICTs– Q4 2011 (report)
Good Practices on Interconnected Networks – Q4 2011 (report)
Recommendations on the security and resilience of SCADA systems – Q 4 2011 (report)
Good Practices on mutual aid assistance and co-ordinated response and recovery measures - Q 4 2011 (report)

STAKEHOLDERS

Authorities in Member States dealing with Resilience and CIIP issues (e.g. national regulatory authorities, ministries, CERTs, dedicated agencies),
Telecommunications and Energy Providers (fixed, mobile and IP-based)
Internet Service Providers (ISPs)
Banks
Sector associations

RESOURCES FOR 2011 (person months and budget)

- 22,5 person months
- 150 kEuro

LEGAL BASE

ENISA regulation article 3
EC CIIP communication COM(2009) 149 (chapter 5.1, 5.2, 5.3)
Council Resolution 2009/C 321/01 (article VIII)
Digital Agenda (chapter 2.1, 2.3)

3.2.3 WPK 2.3: Secure architectures & technologies

WS Name

WS2: ENISA as competence centre for securing current & future technologies

WORK PACKAGE NAME :

WPK 2.3: Secure architectures and technologies

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals)[17]:

SMART goal: At least 5 sector actors (i.e. representatives of industry, regulators, academia, etc.)validating the report on the use of advanced cryptographic techniques, through contributions in the review process, participation in relevant WG's, quotations and references in publications, etc.	**KPI:** # Sector Actors
SMART goal: Coverage of at least 150 M users by operators surveyed in the study on the expectations and deployment status of technologies by network operators	**KPI:** # Users
SMART goal: At least 5 sector actors (i.e. representatives of industry, regulators, academia, etc.)validating the study on technologies with potential to improve the security of the internet infrastructure, through contributions in the review process, participation in relevant WG's, quotations and references in publications, etc.	**KPI:** # Sector Actors

DESCRIPTION OF TASKS:

In its proposal, for a European Digital Agenda the European Commission is aiming towards "building people's trust in using the Internet", thereby creating conditions for the Internet ecosystem to flourish. This can be achieved on one hand by safeguarding the integrity of information, protecting the source of information and protecting personal data, securing the privacy of the individuals[18], while on the other hand protecting the underlying network infrastructure and supporting services. At the same time this effort is taking into consideration and aligns itself with the associated regulatory framework in the EU, in particular the Directive 2002/58 on Privacy and Electronic Communications (also known as ePrivacy Directive) and the Telecommunications Package Reform.

Between 2008 and 2010 ENISA studied the potential of several technologies (IPv6, MPLS, DNSSEC, secure routing) in improving the internet infrastructure (in terms of its resilience characteristics), but also in terms of how this potential was perceived by network operators and of their deployment status. During 2011, ENISA aims to examine the deployment status of these technologies and, in certain cases, to support deployment This support will be realised through the development of Good Practice Guides, Security Guidelines, etc. in wide cooperation with stakeholders. This work will be complemented with relevant dissemination activities in an effort to bridge the gaps between the technical activities carried out with the deployment community and the end user perception,

Complimenting this work, any gaps in terms of technology identified will be used to provide input to proposals that will be made to the Commission for the launch of security standardisation activities.

17 Since the reports that will be the outcome of this activity will be published during Q4/2011 assessment of the relevant KPIs should be carried out in the period of Q2-Q3/2012.

18 For an overview of the work proposed by ENISA on Privacy and Trust please refer to WPK3.2

Moreover, capitalising on the cooperation with stakeholders, the Agency will examine the feasibility of producing an annual report on threats to the internet infrastructure. Such a report would identify and quantify the threats that affected the operation of the Internet during a given timeframe, together with their impact. In addition, it would follow the development of technologies and mitigation measures for those threats. During 2011 will be restricted to two areas where the Agency has already established working partnerships with key sectors actors (DNS and secure routing).

Supply chain integrity in the ICT industry is a topic that receives attention from both the public and private sectors. Currently, it is addressed separately in different industries. Important solutions have been developed in various areas of ICT, which have led to considerable progress and highlighted the need for a comprehensive research study dealing with supply chain integrity. ENISA will study the good practices among various industry segments, investigating feasibility of bridging the gaps in developing common guidelines.

Loss of confidentiality of information is another important area. Since unauthorised information disclosure is difficult to eliminate, a tangible alternative is to reduce the amount of stored and processed identifiable information, which diminishes the privacy risks by reducing the quantity of information exposed. In this light, the research community has already put forward proposals where data are decentralising using advanced cryptography, keeping personal data rather locally than in multiple centralised databases. The main disadvantage of these solutions is the extra cost associated to advanced cryptographic solutions. In 2011 ENISA aims to investigate and evaluate the available solutions making practical recommendations to the EU policy makers.

OUTCOMES AND DEADLINES:

- Update of the ENISA studies on technologies with potential to improve the security of the internet infrastructure (Q4/2011)
- Review of the expectations and deployment status of technologies by network operators (Q4/2011)
- Study on the use of advanced cryptographic techniques in Europe (Q4/2011)

RESOURCES FOR 2010 (person months and budget)

- 13,5 person months
- 90 kEuro

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, Article 1.2

3.2.4 WPK 2.4: Early warning for NIS

WS Name

WS2: ENISA as competence centre for securing current & future technologies

WORK PACKAGE NAME :

WPK 2.4: Early warning for NIS

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: By Q4 2011, at least 10 references to each report or toolset from external websites, official publications, discussions on mailing lists or other means.

KPI: # of references

DESCRIPTION OF THE WORK PACKAGE

This activity in general relates to "early warning" and situational awareness in the Internet. The activity is two-fold: the first part aims at enhancing the capability of CERTs to keep them informed, the second part involves timely information sharing and alerting of constituents of CERTs, with an emphasis on citizens and SMEs.

The first activity in this package will examine the area of good practice for situational awareness for CERTs. In a first round an analysis of available "early warning" mechanisms (like sensor networks, open source information monitoring, etc.) will be made, in order to define the state of the art of "early warning" for NIS. The results will be further processed, the benefits and shortcomings will be assessed and potential further developments in order to improve "early warning" will be outlined. In addition, if applicable, a step-by-step description on how to proceed with the planning and implementation of "early warning" systems in practice will be derived.

The second activity will focus on engaging MS and their Gov/National CERTs and response capabilities in implementing the EISAS roadmap produced in 2010. The main outcome will be a ready-to-use package (called "EISAS basic" in the roadmap) for a first easy and quick adoption by the Member States, and a more detailed plan on how to further support the Member States in deploying an enhanced version of information sharing and alerting. Details see the EISAS roadmap from 2010.

OUTCOMES AND DEADLINES:

First version of "Early Warning for NIS – Status Quo and further development" (Q4/2011)
"EISAS basic" toolset, ready to be used (Q4/2011)
Provisions for "EISAS enhanced" (Report Q4/2011)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

CERT community, Member States institutions, research institutions, etc.

RESOURCES FOR 2011 (person months and budget)

- 13 person months
- 70 kEuro

LEGAL BASE
ENISA regulation article 3
EC CIIP communication COM(2009) 149 (chapter 5.1, 5.2, 5.3)
Council Resolution 2009/C 321/01 (article VI.3 and VIII)
Digital Agenda (chapter 2.3)

3.3 WS3 : ENISA as promoter of privacy & trust

WS NAME :

WS3: ENISA as promoter of privacy & trust

DESCRIPTION OF THE PROBLEM TO SOLVE:

This Work Stream is concerned with promoting information security awareness of economic factors and factors relating to privacy and trust.

On-line services, applications and transactions are expected to bring about considerable benefits and competitive advantage for European citizens and the European economy. However, this can only be achieved if the economic stimuli for developing and using such applications are present and barriers are carefully controlled. At present, there is little data at the pan-European level describing such barriers and incentives. Examples of issues that illustrate this situation are:

- Does the supply of security software match the demand, or better said the needs of the consumers and the industry?
- Do the latter understand their needs in terms of security?
- What is the economic impact of vendor lock-in?
- To what extent is the security market determined by available products?

Similarly, European citizens are unlikely to fully embrace the model of on-line services if certain basic security mechanisms are not present. In particular, future services must guarantee:

- Integrity of the information they handle.
- Protection of the source.
- Genuine authentication (of entities or data, where required).
- Establishment of trust (with persons, as well as objects and actuators).
- Protection of personal data and the privacy of the individuals.

In order to promote advances that are made in these and other areas relating to NIS, Europe currently lacks a structured pan-European approach to raising awareness. Here, lessons could be learned from other economic powers (e.g. the United States, which has established a Cybersecurity month).

DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

There are four work packages in this work stream:

- Understanding and analysing economic incentives and barriers to information security.
- Ensuring that privacy, identity and trust are correctly integrated into new services.
- Supporting the implementation of article 4 of the ePrivacy Directive (2002/58/EC).
- Promoting the establishment of a European Cyber Security month.

The objective of the first work package is to analyse the economic barriers and incentives for improving information security at the pan-European level. Based on existing studies and research into the economics of security, ENISA will analyze economic drivers and barriers in a number of areas (including legal, policy, technical and educational) and will identify potential areas of improvement.

The second package will examine how privacy, identity and trust are integrated into new services and propose recommendations for improvements based on the experience to date. The goal here is to assess and evaluate current developments in protecting the privacy of individuals and in enhancing the level of trust in network services, with a view to developing guidelines for further improvement.

The third work package covers the support that ENISA will provide for the implementation of Article 4 of the ePrivacy Directive. This work is a continuation of the collaboration with Art.29, the EDPS as well the European Commission (DGs JUST and INFSO) and has as its objective to investigate how to practically implement at EU level the provisions of Article 4.

Finally, ENISA will work with Member States to see to look into the possibility of organising a European Cybersecurity month.

WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

This work stream supports the following high-level goals:
Provides Member States with pan-European data on the economics of security.
Assists Member States in establishing a framework for managing privacy and trust.
Facilitates a pan-European approach to awareness raising on NIS issues.

STAKEHOLDERS + BENEFICIARIES

EU Institutions
Private Sector
Member States.

WHY ENISA?

ENISA has already developed a core competency in this area and has facilitated the creation of an Awareness Raising Community that is both able and willing to share experience in coping with emerging issues.

3.3.1 WPK 3.1: Identifying and promoting economically efficient approaches to information security

WS Name

WS3: ENISA as promoter of privacy & trust

WORK PACKAGE NAME :

WPK 3.1: Identifying and promoting economically efficient approaches to information security

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: By end of Q4 2011, at least 50 downloads of each report

KPI: # of download

DESCRIPTION OF TASKS:

Based on existing studies and research into the economics of security (e.g. , study commissioned by DG-INFSO entitled "SMART 2007/2005, Survey and Analysis of EU ICT Security Industry and Market for Products and Services", http://www.formit.org/smart/) ENISA will analyze economic drivers and barriers in a number of areas (including legal, policy, technical and educational) and will identify potential areas of improvement to boost security and resilience in public systems and networks and consequently to relevant products. At the same time, this effort contributes to the identification of security requirements, particularly in public procurement for ICT products and services. In this way, this work package contributes to the points announced in the Digital Agenda for Europe.

The approach followed within this work package will be as follows:

A - Summarize existing knowledge
There is already debate at the international level on these issues, which has resulted in several studies and analyses. ENISA will collect and analyze the existing knowledge available in order to avoid duplication of work. To some extent, this work package can be considered as a logical follow-up to the study commissioned by DG-INFSO entitled "SMART 2007/2005, Survey and Analysis of EU ICT Security Industry and Market for Products and Services".

B - Identify concrete areas of concern and make recommendation
Once the analysis exercise has been completed, ENISA will identify key issues that need to be addressed in the short term. As part of this work, ENISA will identify particular stakeholders affected by this challenging environment, such as the consumers, industry and state. We will then identify and analyze the ways they are affected and possible ways to address their concerns.

In order to do this effectively, we will establish a multidisciplinary working group, comprising of economists, legal experts, sociologists, representatives of consumer organizations and industry bodies.

OUTCOMES AND DEADLINES:

- List of recommendations for methods to better balance supply and demand. Final recommendations to be provided in Q4 2011 (report)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Member states, Industry, consumer organisations, other multipliers

RESOURCES FOR 2011 (person months and budget)

- 14,5 person months
- 50 kEuro

WORK PACKAGE PROPOSED BY:

ENISA, DG-INFSO

LEGAL BASE

ENISA regulation article 3
Digital Agenda (chapter 2.1, 2.3)

3.3.2 WPK 3.2: Deploying privacy & trust in operational environments

TP Name

WS3: ENISA as promoter of privacy & trust

WORK PACKAGE NAME :

WPK 3.2 : Deploying privacy & trust in operational environments

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals)[19]:

SMART goal: At least 5 sector actors (i.e. representatives of industry, regulators, academia, etc.) validating the report on minimal disclosure, through contributions in the review process, participation in relevant WG's, quotations and references in publications, etc.	**KPI:** # Sector Actors
SMART goal: At least 5 sector actors (i.e. representatives of industry, regulators, academia, etc.) validating the report on trust and reputation models, through contributions in the review process, participation in relevant WG's, quotations and references in publications, etc.	**KPI:** # Sector Actors

[19] Since the reports that will be the outcome of this activity will be published during Q4/2011 assessment of the relevant KPIs should be carried out in the period of Q2-Q3/2012.

SMART goal: At least 5 sector actors (i.e. representatives of industry, regulators, academia, etc.) validating the report on monetizing privacy, through contributions in the review process, participation in relevant WG's, quotations and references in publications, etc.

KPI: # Sector Actors

DESCRIPTION OF TASKS:

On-line services, applications and transactions can assure benefits and competitive advantage for citizens and European economy. However, this cannot be achieved without safeguarding the integrity of the information, protection of the source of information, the genuine authentication (of entities or data, where required), establishment of trust (with persons, as well as objects and actuators) and at the same time protecting the personal data and securing the privacy of the individuals.

This activity seeks to ensure that Europe can effectively manage the introduction of new services with a high level of security while at the same time limiting the threats to civil liberties and privacy. This can be achieved by:

- Advocating and fostering a Pan-European approach to privacy;
- Proposing new models for trust-establishment;
- Developing guidelines for regulatory review and interpretation.

The proposed activity is fully in line with the aims of the Digital Agenda. Furthermore, the work carried out will taking into consideration a number of activities/initiatives that take place at International level, namely:

- The Future Internet (FI) Assembly (FIA) and Private Public Partnership (FI PPP)[20];
- The Research & Innovation on Security, Privacy and Trustworthiness in the Information Society (RISEPTIS) report and the conclusions of the Conference on 'Trust in the Information Society', 10-11/02/2010.
- The associated regulatory framework - in particular Directive 2002/58 on Privacy and Electronic Communications (also known as ePrivacy Directive) and the Telecommunications Package Reform.

The activities foreseen for 2011 are as follows:

Promoting a pan-European approach to privacy and trust-establishment models

20 A public-private partnership on the Future Internet. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 28 October 2009 http://ec.europa.eu/information_society/activities/foi/library/fi-communication_en.pdf

Based on the results obtained in 2010 in the area of ID management, in 2011 ENISA aims review the issues of anonymity and network 'forgetfulness' of the users identity information, with the objective of producing guidelines for policy makers. Privacy Enhancing Technologies (PETs) rely on confidentiality of personal data and anonymous communication to support their privacy assumptions. However the current context given by surveillance capabilities allows linking individuals with their 'traces' in Information systems. Linking of different information items relating to a person, which in isolation would not constitute personal data, should be considered as well when defining data protection. In this context, a concept that is gathering interest in the research community is minimal disclosure. ENISA will study available and emerging methods of preserving the privacy by providing only the most needed information of users to the service providers. Initiating such a process of defining levels of privacy for a certain type of applications could trigger development of criteria for minimal identifiable information to be used. In addition, privacy versus security issues, reflecting potentially different requirements and exposing different interests (in particular regarding different stakeholders etc) will be addressed.

An increasing number of online services rely on reputation based systems; decision supporting systems have impact on the quality and trust perceived by the users. The robustness of such systems is essential as they have economic impact. However, privacy aspects are not yet considered in the design of reputation systems. Some privacy-preserving/-respecting online reputation systems have been proposed by the research community. For example, anonymity has been deployed in payment systems and can serve as model for other online systems. Liveliness has been considered in order to allow negative voting and updating of reputation based on the recent behaviour, avoiding accumulation of rating. An evaluation of different reputation based trust models addressing their privacy, anonymity and liveliness characteristics is required.

Supporting the EC Action Plan on e-signatures and e-identification

Since 2009 the European Commission is working towards the creation of a comprehensive electronic identification, authentication & signature framework consisting of a number of flagship actions at EU level, summarised below:

- Rationalisation of eSignature standards via means of an EC standardisation mandate;
- Update Decision 2003/511/EC
- "Trusted List" of Qualified Certification Service Providers
- eSignature formats
- Supervision of qualified certificates providers

During 2011 the EC is expected to prepare the draft text proposal of its action plan where ENISA will assist and support the Commission Services.

Monetising privacy

An important area of work that is 'horizontal' in support of this activity is that of Monetising Privacy. Until today most online service offers are free and based on targeted advertising. In the Future Internet it is important to establish confidence between the EU citizens, businesses and the services offered. This will be achieved through sharing of revenues among all actors of the business chain and also via ensuring that users maintain full control over the ownership of their data within networked systems. In this light, assessing what is a fair price of a user's profile and how this may vary if this user (profile) is considered as a part of a group ('bargaining power of individual') are important elements supporting this work as well as of policy makers in this area. Finally, ENISA aims to put forward for the consideration of policy makers the use of alternative (to the existing and mostly used free) service models for online services. As examples prepay or subscription based systems will be considered.

OUTCOMES AND DEADLINES:

- Report on minimal disclosure and other principles supporting privacy and security requirements (Q4 2011)
- Report on trust and reputation models. Evaluation and guidelines. (Q4 2011)
- Study on monetizing privacy (Q4 2011).

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

European Institutions.
Public institutions in Member States deploying eID.
Private sector representatives involved in supporting eID initiatives.

RESOURCES FOR 2010 (person months and budget)

- 14 person months
- 164 kEuro

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

European Digital Agenda,
Directive 2002/58 on Privacy and Electronic Communications, (the ePrivacy Directive)
The Telecommunications Package Reform

3.3.3 WPK 3.3: Supporting the review and implementation of the ePrivacy Directive (2002/58/EC)

WS Name

WS3: ENISA as promoter of privacy & trust

WORK PACKAGE NAME :

WP 3.3 : Supporting the implementation of the ePrivacy Directive (2002/58/EC)

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: At least 5 sector actors (i.e. representatives of industry, regulators, academia, etc.) validating the study on extending the obligation of notifications about data breaches, through contributions in the review process, participation in relevant WG's, quotations and references in publications, etc.[21]	**KPI:** # Sector Actors
SMART goal: Representatives of 10 DPAs from EU MS attend the workshop	**KPI:** # DPA's

DESCRIPTION OF TASKS

In 2010, ENISA in collaboration with the European Data Protection Supervisor (EDPS), the European Commission and members of Art.29 carried out a review of the current situation concerning the introduction of a European data breach notification requirement for the electronic communication sector that was introduced in the review of the ePrivacy Directive (2002/58/EC)[22].

The main objective of this work was the development of a consistent set of guidelines addressing the 'implementation measures' and procedures as described by Article 4 of the ePrivacy Directive. An overview of the first results of this work was presented during the 76th meeting of the Data Protection Working Party of Article 29 (July 2010) where many representatives of DPA' in the EU expressed their support.

In 2011 ENISA aims to continue this collaboration with Art.29, the EDPS as well the European Commission (DGs JUST and INFSO) with the aim to investigate how to practically implement at EU level the provisions of Article 4. In this respect a workshop will be organised in Brussels (late January) in collaboration with the EC and EDPS with the aim to:

21 Since the reports that will be the outcome of this activity will be published during Q4/2011 assessment of the relevant KPIs should be carried out in the period of Q2-Q3/2012.

22 Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

1. Present the final results of ENISA's 2010 work,
2. Invite a number of industry representatives to present their views, and
3. Get feedback in the areas where ENISA could contribute.

From the work conducted so far it is evident that one of the main hurdles to overcome is the divergence of views between DPA's and industry. In this light, ENISA will try to put forward proposals that address the concerns of both sides. A set of recommendations regarding the implementation of the obligation of notifications (with particular attention on the topic of risk assessment of data breaches) will be proposed. As was the case in 2010 this work will not only address the telecommunications sector (referred to as eComms sector in Directive 2002/58/EC) but also other sectors such as the finance sector, healthcare, etc. where the implementation of the ePrivacy Directive is expected to have significant impact.

OUTCOMES AND DEADLINES:

Workshop on data Breach Notification (Q1/2011)
Study with recommendations on the implementation of the obligation of notifications about data breaches (Q4/2011)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

European Institutions (Commission, EDPS)
Article 29 working group.
Data Protection Authorities within Member States

RESOURCES FOR 2011 (person months and budget)

- 11 person months
- 40 kEuro

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3b), c), d), f), g) and k)

3.3.4 WPK 3.4: European Cyber Security Awareness Month

WS Name

WS3: ENISA as promoter of privacy & trust

WORK PACKAGE NAME :

WPK 3.4: European month of network and information security for all

DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):

SMART goal: By end of Q4 2011, at least 50 downloads of each report	**KPI:** # of download
SMART goal: At least 50% of the EU population is represented at the workshops	**KPI:** % of EU population represented
SMART goal: Event participants score the event at least as 3 on a scale of 1-5	**KPI:** Average feedback on scale of 1-5

DESCRIPTION OF TASKS:

In today's digital world, we rely more and more on computer networks and information systems for our daily activities. The extensive use of the internet makes our life easier but at the same time it exposes users to security and privacy risks. This exposure poses challenges for the protection of involved values that are subject to cyber attacks. In order to achieve a high level of security in the cyber world, we need to involve not only institutional actors like public sector bodies and private sector companies but also and most importantly the end users.

As already foreseen in the proposal of the new ENISA regulation, ENISA shall be involved in organising, in cooperation with the Member States, the **'European month of network and information security for all,'** featuring national/European Cyber Security Competitions. Within this work package, we would like to elaborate on the structure, organisation modalities, coordination effort and thematic coverage of Europe wide events (i.e. Member States, EFTA countries, and candidate countries) with the objective to foster a security culture. Both the feasibility and details of such an event will be in focus.

The idea was inspired by similar projects that are being held successfully in other places of the world for some years now. We figure that this project will raise significantly the awareness of the EU citizens on NIS issues. The campaign is addressed mainly to the end users, being the catalyst in achieving a high level of cyber security. Thus, the main concept is to bring basic ideas, tips and practices on NIS to the general public.

The particularities of the European territory compared to other areas in the world (e.g. multilingual environment, sovereign member states etc) suggest that a significant amount of effort will be required in order for this idea to deliver its full potential across Europe. To this effect, one of the most critical elements for the success of this campaign is to develop an effective structure and coordination scheme among participating entities.

We believe that ENISA is ideally positioned for the role of facilitator and coordinator of such a campaign. In order to maximise its impact, we aim to involve the national governments of the member states as much as possible in all phases of the development. Among other possibilities we might consider establishing a Cyber Security Awareness Month partnership with creating synergies and mutual benefits at international level. We will also make use of existing networks and amplifiers (e.g. ENISA Awareness Raising Community, AR Group for EU Institutions etc)

By Q1 of 2011, we expect to have established cooperation with other public bodies that organise similar campaign for some years now, in order to obtain valuable input based on their experience. We will examine the best practices applied so far worldwide and we will focus on those that can be better accommodated in Europe. Following the exchange of views and knowhow, and with the involvement of Member States we will assess the feasibility and explore various options on how such a campaign can become an effective instrument to raising awareness about NIS challenges and in particular:

- Generate awareness about NIS
- Involve relevant stakeholders
- Disseminate security relevant information
- Coordinate their activities internationally

OUTCOMES AND DEADLINES:

- Report on the structure, organisation modalities, coordination effort and thematic coverage of Europe wide events in Q4 2011.
- We aim at presenting the results of this work within an inauguration event in Q4 2011.

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Member states, European Commission

RESOURCES FOR 2011 (person months and budget)

- 15 person months
- 50 kEuro

WORK PACKAGE PROPOSED BY:

ENISA, DG-INFSO

LEGAL BASE

ENISA regulation article 3
Digital Agenda (chapter 2.1, 2.3)

3.4 Summary of Work Streams and Work Packages

WS1	ENISA As a Facilitator For Improving cooperation	Budget line	Budget	Person months
WPK1.1	Supporting Member States in implementing article 13a	3510	150.000	19,5
WPK1.2	Preparing the Next Pan-European Exercise	3510	140.000	21,5
WPK1.3	Reinforcing CERTs in the Member States	3300	26.000	10
WPK1.4	Support CERT (co)operation on European level	3300	160.000	21
WPK1.5	CERTs role in supporting the fight against cybercrime	3300	120.000	16,5
			596.000	**88,5**

WS2	ENISA As a Competence Centre For Securing Current & Future Technology	Budget line	Budget	Person months
WPK2.1	Security & privacy of Future Internet technologies	3520	80.000	31,5
WPK2.2	Interdependencies and interconnection	3510	150.000	22,5
WPK2.3	Secure architectures & technologies	3520	90.000	13,5
WPK2.4	Early warning for NIS	3300	70.000	13
			390.000	**80,5**

WS3	ENISA As a Promoter of Privacy & Trust	Budget line	Budget	Person months
WPK3.1	Identifying and promoting economically efficient approaches to information security	3330	50.000	14,5
WPK3.2	Deploying privacy & trust in operational environments	3520	164.000	14,5
WPK3.3	Supporting the implementation of the ePrivacy Directive (2002/58/EC)	3520	40.000	11
WPK3.4	European month of network and information security for all	3330	50.000	15
			304.000	**55**

Total			**1380.000**	**224**

MISS	Missions Operational Departments (TCD)	3013	288	

4.1 Introduction

Engaging and advancing dialogue between public and private sector actors are at the heart of ENISA's mission. In 2011, this will consist of the following activities:

- Management of ENISA's formal bodies (the Management Board and Permanent Stakeholders Group, or PSG)
- Establishment and subsequent management of informal NIS Stakeholder and National Contact Officers (NCO, former NLO) networks;
- Establishment of a platform for managing stakeholder contacts.
- Continued consultation with key stakeholders and follow-up within the project lines.

Through close alignment with internal technical activities and with national and EU strategies, these activities with public and private stakeholder will enhance the value of ENISA's Strategic and Public Affairs communications and the identification, production and development of good practices within the Work Programme.

In 2011, stakeholder engagement will focus on developing a more effective stakeholder dialogue in each of the work streams described in the previous sections.

Stakeholder engagement, community development, cooperation and exchange of good practices will be deepened and enriched in 2011 by implementing an approach to stakeholder engagement that is closely integrated with the ongoing project activities.

4.2 Management Board

The structure of ENISA's Management Board is laid down in the Agency's founding Regulations. As in previous years, two formal meetings will be organised; in 2011, joint informal meetings of sub-groups will be held with the PSG as appropriate. In addition, more active direct communication (e.g. by means of a forward-looking electronic newsletter) and more focused working with sub-groups of different MS organised to focus on particular issue areas is to be proposed in 2010. In 2011, these efforts at improving communication and adding more targeted value to identified sub-groups of MS will continue through inter-active portal-based communities of interest.

KPIs: 2 formal meetings; 1 informal meeting; 1 joint MB/PSG meeting; 4 electronic newsletters.

4.3 Permanent Stakeholders Group and NIS Stakeholder networks

Members of the PSG primarily act as advisors to the Executive Director. In addition to their well-established role in advising on the overall content and orientation of the work programme in 2010 they will also be developed as promoters for ENISA WP activities, as leaders of identified sub-groups of NIS Stakeholder network communities and as sources of advice on experts for TCD expert groups. In addition, more active direct communication (e.g. by means of regular forward-looking electronic newsletters) and more focused working with sub-groups of different NIS Stakeholder communities on particular issue areas is to be proposed in 2010.

In 2011, as in the past, two formal meetings will be organised; in 2011, joint informal meetings of sub-groups will be held with the Management Board as and when required. Improved leadership and communication capabilities for identified sub-groups of NIS Stakeholder network communities will continue through the development of inter-active portal-based communities of interest and face-to-face meetings around specific issue areas (particularly in relation to public-private cooperation) with NCON members.

KPIs: 2 formal meetings; 4 electronic newsletters.

4.4 National Contact Officers Networks (NCONs)

Beside the official bodies of the MB and the PSG (which are specified by the ENISA regulation), contacts to national bodies to support the day to day work are established. In 2011, the previous NLO network will be expanded to include more differentiated networks of general policy and specific regulatory contacts developed, in order to create something that fits more closely with the various interests of our different Member States and that is more flexible in responding to their evolving needs and the changing requirements of EU network and information security.

It should be noted however that the NLOs will continue to play the role of a single point of contact in Member States. But more structured ongoing contact will be developed with personnel in national regulatory agencies and the range of government ministries with whom we already either have to or do interact but on a sporadic and piecemeal basis. To signify this expansion of a single NLO network to more diverse ones we are proposing the term National Contact Officers Networks (NCONs), which will be established on a non-permanent, ad hoc basis. We envision organising small meetings of a limited number of NCOs according to the particular interests of different groups of MS. We would expect these meetings to discuss (perhaps even develop themselves) and agree particular work programme activities, and then to validate/approve outcomes. To ensure that the creation of NCONs is an ordered and transparent process for the MB, we intend to report on proposed NCON meetings to the MB on a regular and ongoing basis.

In addition to broad organisational desiderata, events such as implementation of Article 13 of the revised Telecoms Directive, and Article 3(d) of the e-Privacy Directive, are driving us in this direction and we expect will be a particular area of focus in 2011.

KPIs: NCON meetings involving between 5 – 12 Member States representatives each.

4.5 Stakeholder Relationship Management (SRM) platform

ENISA seeks to revise its stakeholder strategy and shift towards a collaborative approach investing in reciprocal, evolving and mutually defined stakeholder's relationships. Moreover, by grasping the need for refocusing its efforts ENISA is migrating from the concept of managing stakeholders to collaborating with the stakeholders. This is achieved by positioning the activity in the nucleus of the technical competence of the Agency. This tactical realignment is in line with the need of the agency to have an integrated and focussed approach that will aim in building relations with NIS stakeholders in a coherent manner driven by the agency's mission, strategy, and work programme while respecting its regulatory framework of operation.

In view of enchasing ENISA's capability for sharing knowledge and stimulating debate with its stakeholders the Agency will asses solutions in order to provide an information exchange and knowledge sharing platform for the key stakeholders from across Europe.

The primary goal for 2011 will be to identify through collection of requirements the appropriate tool to be used in addressing the identified needs in stakeholder management. Further to the collection of requirements a wide range of options will be assessed in order to identify the most suitable effective and efficient Stakeholders Relationship Management (SRM) platform that will best serve the envisaged purpose.

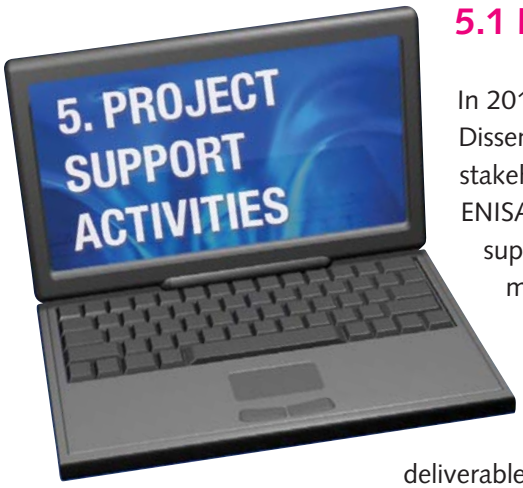
4.6 Consultation and follow-up

ENISA's focus for external relations is on actively engaging, consulting and listening to its constituents hence building its credibility and reputation as a point of reference for Network and Information Security in Europe. External Relations activities will support the efforts of the technical competence of ENISA to increase outreach capabilities and further enhance the efforts of the Executive Director for increased visibility of the Agency and its activities in a very crucial year for ENISA's future mandate.

External Relations will seek to incrementally support the efforts of several functional areas of the Agency for the ongoing development of relationships with Member States, EU Bodies, industry, academic and consumer representatives, Third Countries and International Institutions (e.g., ITU, IETF and OECD) and explore the possibility of supporting Public-Private Partnerships (PPPs) that bring together these different actors. This activity as last year will be implemented in close cooperation with the European Commission and should be seen as a continuation of the horizontal activity introduced in the work program 2010. These activities will mainly be implemented through the mission budget for enhancing the presence and interaction of a number of ENISA actors with our NIS and policy constituents.

4.7 Summary Table

Activity	Stakeholder Relations	Budget line	Budget	Person months
SR1	Management Board	3003	110.000	2,5
SR2	Permanent Stakeholder Group & NIS Stakeholders	3000	90.000	2,5
SR3	National Contact Officers Networks	3320	20.000	2
SR4	Stakeholder Relationship Management Platform	3330	80.000	19
SR5	External Relations	N/A	N/A	2
Total			**300.000**	**28**
MISS	Missions Operational Departments (SR)	3013	45.000	



5.1 Promotion and Dissemination activities

In 2011 ENISA aims to move to a new approach on Promotion and Dissemination of its deliverables based on the emerging needs of stakeholders and the evolving work of TCD. Under this new concept ENISA sees to organize Promotion and Dissemination as a project support activity with a primary objective to promote ENISA's work more effectively.

Promotion and Dissemination will be involved in the operational activities at an early stage in order to identify the stakeholders' groups that are mostly interested for each of the agency's deliverables. In that way, there will be better and timely planning for the promotion of ENISA's output.

In cooperation with the external relations activity, there will be a continuous matching process between the work of ENISA and the respective interested parties (i.e. mapping of stakeholders). Moreover, this activity may involve analyzing and re-synthesizing parts of the ENISA deliverables in order to address more effectively specific needs of certain stakeholders.

ENISA will be strengthening the collaboration with Member States in these activities, in order to ensure a prompt dissemination of information best meeting the expectations of the Member States and other relevant stakeholders. This will be performed in a way that amplifies the impact of the produced deliverables.

At the same time, Promotion and Dissemination will promote the ENISA brand name, building the image of the agency among its stakeholders. Furthermore it is expected that a dissemination policy will be embedded in the projects from the preparation process of the work program of the agency as part of the overall integrated process.

In particular, we see the following tasks within Promotion and Dissemination activities:

- Support TCD in implementing the ENISA dissemination strategy and approach in line with the stakeholder's analysis and mapping. This should be an intergraded approach also with the projects.
- Support TCD in disseminating ENISA deliverables to the respective stakeholders. The approach should be linked and follow the outcome of stakeholder's analysis and mapping.
- By ways of Dissemination on a horizontal way enhance the ENISA brand and the NIS European corporate identity to a multilayer of stakeholders. This should be also an intergraded approach with the projects and PAU.
- Provide horizontal service and support to ENISA for dissemination activities at all operational levels.
- Promote ENISA deliverables through dedicated slots at the 2011 Summer School on Network and Information Security jointly organized by ENISA and FORTH.

5.2 Integrating NIS into education

It is well recognized that the interaction of the younger generations with computers and the internet begins nowadays at very early stages of their sensitive youth. Therefore it is of paramount importance and of significant added value to pursue such activities through the appropriate mechanisms that would establish new and enrich existing IT curriculum topics that would raise awareness and enhance the NIS culture of the users from the early steps of their interaction and exposure with the digital reality. Integrating NIS into education is a key part of developing an NIS risk oriented culture by teaching children and young adults about network and information security. Cultivating informed and aware generations by embedding NIS risk posture into their way of life and on-line behavior will enhance the development of a mature and conscious society in their interaction with the digital world.

Creating a security culture does not have to start after entering into the world of work, as it is the case now; NIS risk posture and security culture should be taught at an early age so that young people will have already integrated the appropriate notions into their skills. Education about NIS should therefore be part of the school curriculum for young people and of the vocational training of young professionals. ENISA should see to perform stock taking activities in the respective area in order to identify existing best practices of information channeling into the national educations schemes. To this respect ENISA aims to liaise and cooperate with the appropriate Commission services (DG INFSO, DG EAC), European Agencies in the field (Cedefop, ETF) and the Member States in view of coordinating activities and achieving synergies that would result to a greater impact
This activity is positioned within the horizontal activities as it draws from various other TCD activities/output such as, stakeholders, awareness, deliverables, and NIS good practices. Furthermore, this activity aims to support the overall goal of ENISA to disseminate objective and comprehensive information on network and information security issues for all users in line with Article 2(e) of the founding regulation (see also Dissemination Strategy below).

5.3 Risk Management activities

Risk Management and Risk Assessment are vital parts for when coping with information security. For most NIS activities, assessment of relevant risks and the establishment of the respective risk management plan is of paramount importance in order to produce quality results thus providing respective assurance to the respective stakeholders. As of 2011, the Agency has recognized the need for a horizontal integration of risk assessment and risk management in the operational activities of ENISA. Therefore capitalizing on the existing expertise, gained experience, achieved results, recognition and good practices that have been acquired by ENISA during the past years the Agency will deploy the risk assessment activity as a horizontal service embedded into the relevant operational activities.

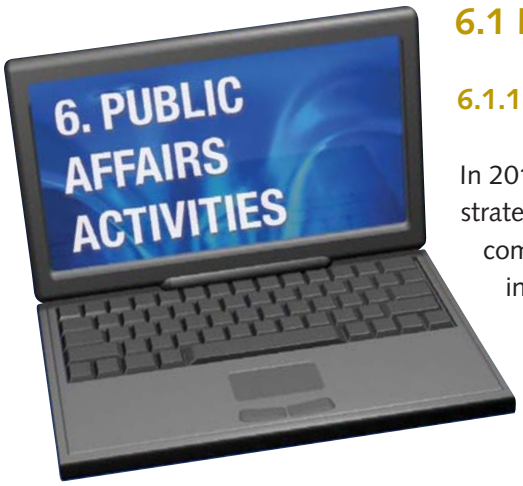
By developing a set of tools and an information repository ENISA will progressively establish the following support services that were deem appropriate, would enhance the completeness of the operational output:

- Provision of guidelines and tools to perform risk assessments
- Provision of guidelines to perform identification of emerging and future risks
- Provision of data/knowledge from previous ENISA assessments by means of a repository of threats, assets, vulnerabilities, controls, etc.
- Provision of a mechanism to expand available repository from future risk assessments
- Assistance in risk assessment issues required within ENISA activities on demand

The received feedback from the various activities will be integrated into the available repository for future use. Based on the knowledge base, conclusions and lessons learned from horizontal Risk Management activities will be summarized by means of a report that will be produced on an annual base.

5.4 Summary of Project Support Activities

Activity	Horizontal Activities	Budget line	Budget	Person months
PS1	Promotion & Dissemination Activities	N/A	N/A	13,5
PS2	Integrating NIS into Education	3330	10.000	4
PS3	Risk Management Activities	N/A	N/A	8
Total			**10.000**	**25,5**



6.1 Public Affairs activities

6.1.1 Introduction

In 2011, the Agency will continue increasing visibility with key actors at strategic and decision-making level and reaching out to NIS communities to promote its work and to enable actors to make informed decisions in NIS matters. The Agency's external communication portfolio is complemented by enhancing its internal communication activities.

6.1.2 Aligning to the Policy Environment

ENISA shall maintain its capability of assessing NIS related technical and political challenges, the general policy environment, threat landscape, market technologies, and needs of its stakeholders in order to be able to adjust its priorities and work accordingly. The Agency's strategic approach shall be developed in close consultation with its stakeholders, including the EU Member States, the European Commission, the Agency's Management Board and Permanent Stakeholders' Group.

ENISA continuously monitors and takes account of all NIS areas with a view to advance ENISA's positioning in relation to the given policy context. This results in media and events activities in line with the advocacy and positioning of the Agency vis-à-vis key stakeholders.

The Agency's annual work programmes shall be aligned to the given European Union policy framework and environment ensuring coherence and continuity in the Agency's short- and medium-term.

According to Art. 10 of the ENISA Regulation, the Agency shall maintain the capability to reply to requests posed by the European Parliament, the European Commission and by notified bodies of the Member States.

6.1.3 Public Relations

The Agency will continue raising its profile as to achieve an increased impact and influence. Increasing visibility and awareness with key actors at strategic and decision-making level is key to live up its regulation based mission to 'enhance the levels of security in Europe'. This includes, among other things, developing and maintaining a network of key actors, participating in relevant fora, organising high-level meetings and participating in high-level events (e.g. EU Presidency events).

6.1.4 ENISA Digital Communication

The ENISA corporate website is the Agency's primary external communication channel, and serves also as "business card" to the interested public. The website shall meet the increasing need to communicate effectively with the wider public, stakeholders in general and NIS communities in particular, and to disseminate the Agency's deliverables. The Agency enhances the website from publishing information and providing a number of portals, towards an interactive and collaborative communication platform to empower stakeholders to work with ENISA more effectively and efficiently. The Agency shall strive for providing compelling digital content, such as video clips, and to increase website traffic in general.

6.1.5 ENISA Publications and Brand Materials

Each year, and in accordance with the founding regulation, ENISA publishes a General Report covering its activities of the previous year. Furthermore, the Agency publishes corporate material, such as fact sheets, corporate brochures and leaflets. The Agency has taken the decisive paradigm shift to reduce printed publications. Therefore, the Agency intends to review the existing publications, and consider the best possible online publications, including an electronic newsletter for more frequent and comprehensive outreach to ENISA stakeholders.

To ensure coherent brand communication through all communication channels, the Agency maintains its corporate brand visibility manual and templates. It uses a databank comprising professional images in addition to own photos of events with a view to a coherent audiovisual appearance, across all channels, online, in PPTs, and publications.

6.1.6 Spokesman and Media Relations

The Agency communicates to the wider public through press and media channels. ENISA maintains a network of both general and specialised media contacts across Europe, issues press releases in five languages, conducts interviews, organises press conferences, and monitors media uptake. Media impact shall be increased through targeting key media at Member State level.

The ENISA Spokesperson acts as primary contact for press and media communication.

6.1.7 ENISA Brand Events

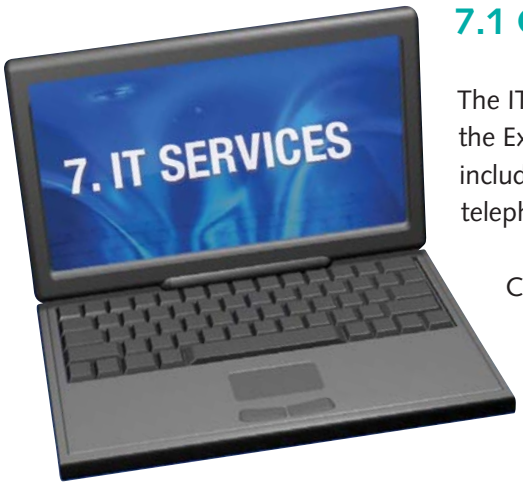
The Agency ensures visibility and disseminates its results at conferences and major political events for NIS and ICT stakeholder communities. ENISA presents itself in Brussels and other major cities with several dedicated events, (e.g.) one being a high-level discussion forum and another being the presentation of the annual General Report. The objective is to contribute to an overall positive appearance and presentation of the Agency.

6.1.8 ENISA Internal Communication

The Agency highly values information sharing and co-operation between its staff and management, and among all staff in general. To this end, ENISA has established various internal communication channels including permanent information sharing platforms by means of its intranet, and organises, among other measures, weekly staff meetings providing an opportunity to raise issues directly by means of face-to-face communication.

6.2 Summary of Public Affairs Activities

PAU	Public Affairs	Budget line	Budget	Person Months
PAU 1	Aligning to the Policy Environment	N/A	N/A	8
PAU 2	Public Relations	N/A	N/A	8,5
PAU 3	ENISA Digital Communication	3220	76.000	8
PAU 4	Publications and Brand Materials	3240	60.000	4
PAU 5	Spokesman and Media Relations	3210	44.000	9,5
PAU 6	ENISA Brand Events	3200	10.000	2
PAU 7	ENISA Internal Communication	N/A	N/A	1,5
Total			**190.000**	**41,5**
MISS	Missions Operational Departments (PAU)	3013	35.000	



7.1 Overview

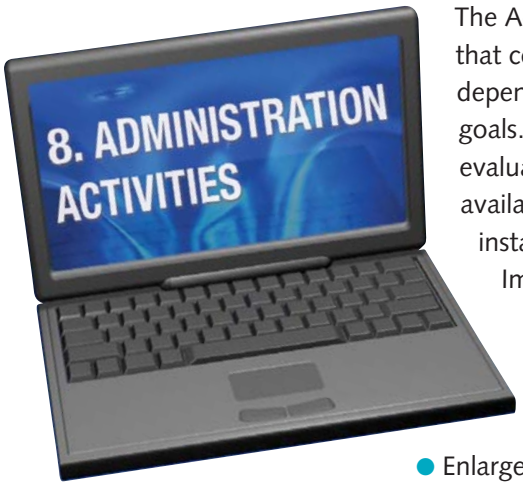
The IT Services Unit (ITSU) is an autonomous unit reporting directly to the Executive Director, delivering ICT services across the agency, including server and desktop computing, IT security, service desk, email, telephony, network storage, printing, Internet and Intranet, etc.

Certain services are outsourced to 3rd parties, e.g. Listserv – discussion / distribution lists (L-Soft) and ABAC Workflow and Assets - financial management systems (European Commission). Application support is also outsourced for several internally running systems.

During 2011 ITSU will focus on the replacement of the current inventory of client computers (> 5 years old); the outsourcing of email, online meeting functionality and web security; the implementation of a new IP telephony infrastructure; the management and maintenance of services, their contractors and agreed service levels; the maintenance of systems, networks, hardware and software; the testing of IT Contingency measures; the enhancement of user productivity through the introduction of additional e-workflows and mobility tools; and finally, the move of all IT related equipment to the new ENISA building.

7.2 Summary of Activities related to IT Services

Activity	Unit	Budget line	Budget	Person Months
ITSU 1	ICT Administration	N/A	N/A	9,5
ITSU 2	ICT Services	2300	60 000	9,5
ITSU 3	ICT Support	2301 2302	130 000	9,5
ITSU 4	Telecommunications	2202	60 000	9,5
			250 000	**38**
MISS	Missions ITSU	3014	5.000	



The Administration Department contributes to the goals of the Agency that concern compliance and assurance; it also makes available dependable services to service administrative as well as operational goals. In 2011 the goals of the Administration Department is to re-evaluate existing services and further expand the electronic workflows available in line with the compliance objectives that have been instantiated in the internal control standards and audit results.

Implementing business continuity goals will also be a priority work item for 2011. In specific in 2011, the Administration Department seeks to:

- Mitigate assurance and compliance risks
- Enlarge the scope of electronic workflows currently in use at the Agency
- Ensure facilities administration and business continuity

8.1 General Administration

General administration tasks contribute to the management and measurement of performance of the Administration Department. Major tasks include planning, advising, representing, reporting upon and controlling the activities of the Sections and the Department.

In 2011 the Administration Department will launch the following projects that aim at improving efficiency in using Agency resources: electronic procurement tool made available for the first time by the Commission (ePRIOR), a tool for contract management (ABAC Contracts), implementation of the business continuity plan and localisation in the specific needs of ENISA and maintenance, outsourced solution for ex-post controls and move to the new ENISA building.[23] These activities are carried out in collaboration with the Agency's IT Services Unit and/or Commission services as appropriate.

In terms of organisational processes, it is expected to extend the scope of ABAC Assets and integrate ABAC with its components in use at the Agency. A significant activity will be associated with the introduction of electronic signatures that will be made available to the Agency by the Commission. The Agency will seek to integrate in this respect XML based and/or pdf forms and electronic signatures to produce signed electronic documents and workflows, further redesigning its current procedures. This activity complements the experience that the Agency has accumulated in redesigning procedures using electronic forms and it will render them more functional and able to serve formal and legal purposes. Additionally it is expected that the General Administration will continue carrying out its role as internal control coordinator and will follow up on audit results concerning audits with an administrative purpose. In 2011 the priorities of General Administration include:

- Mitigate assurance and compliance risks
- Carry out the multi-annual planning of activities
- Monitor annual budget execution
- Re-evaluate services offered (including Hellenic authorities support, missions management etc.)
- Deploy additional electronic workflows
- Ensure business continuity (subject to resource availability)

[23] In 2010 General Administration led such activities as business continuity preparation for the whole Agency, deployment of the electronic workflow for missions' management, preparation of and kick off of the electronic workflow for assets management.

The main activities planned for 2011 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
1.1	Administration activities' planning Representation of AD	Planning of activities, guidance and management. Setting goals and priorities Coordinating with Agency's Departments & Sections Collaborating with key staff to meet service goals People management.	Planning of activities per Section. Guidance to meet goals. Annual work plan. AD staff objectives Coordination. Communication	Ongoing	0
1.2	Advice and support to the ED and Head of Dpts/Units as appropriate on AD related issues, e.g. Governance, sound financial management, activity based management, contingency planning, business continuity, legal services, assets.	Reports to ED and collaborates with the Heads of Departments and key staff as appropriate	Continuous support to the ED and HoTCD, Timely responses to requests for support. Support the implementation of internal controls and systems to control resources and property	Weekly	0
1.3	Ensure that appropriate reporting levels on the use of the Agency's resources are available at all times. Leverage on financial data and AD report lines.	As appropriate	Periodic evaluation of the Department's internal and external reporting needs. Reporting, and follow up.	Quarterly	0
1.4	Follow up on audit results, practices and procedures in line with FR, IR and SR. Collaborate with Internal Control Coordination and Accounting. Business continuity planning. VAT refunds	Update of documents and activities reporting Coordination with internal (Internal Control Coordination, Accounting, Risk Management Section) and external actors (ECA, IAS etc.)	Implement audit recommendations Continuous improvement of performance Risk management	Quarterly	0
1.5	General organisational tasks	Filing, reporting, support to Sections at AD or as appropriate, financial initiation as appropriate	Volume of activities Timely execution	On going	0
1.6	Office services	Administration of horizontal tasks including translations, stationery, logistics, safety & security, post, vehicle, move to a new building, facilities administration.	Volume of activities Timely execution	On going	289.957

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
1.7	Handling requests of Staff members related to the implementation of the seat agreement (special ID cards, car registration, VAT exemption etc).	Regular handling of VAT exemption requests for the Agency's Staff	Number of cases handled Timely responses	Ongoing	0
1.8	Internal control coordination	Liaise with Internal control services of the Commission, most notably the IAS	Number of comments followed up and complied with	On going	0
1.9	Business continuity coordination	Implement the business continuity plan and coordinate with the various ENISA departments/Units and activities involved	Number of actions closed (subject to resources availability)	On going	0
1.10	Events organisation (operational support)	Support the organisation of ENISA events	Number of events organised, punctuality	On going	0

8.2 Accounting and Finance

Accounting at ENISA is a discreet function that addresses the following tasks in line with the financial regulation:[23]

- Annual accounts of the Agency
- Accounting ledgers that include a journal, a general ledger and an inventory
- Validation of systems, assets inventories
- Payments etc.
- Coordination of Audits, most notably with the European Court of Auditors.

Finance carries out budget planning, administration and financial control, portions of payroll administration and missions' overview and back up. The goal of the Finance Section is to ensure the credibility of financial circuits and budget planning. Close monitoring of Budget planning and execution allows the Agency to increase its Budget utilisation rates to the benefit of its operations and counterbalance budget constraints. In 2011 the priorities of the Finance Section include:

- Budget planning including activity based budgeting
- Monitoring of budget execution and planning
- Functional support regarding electronic workflows (ABAC, missions' management)

24 Accounting comprises of the tasks of the Accounting Officer, which is an as independent function that is supervised directly by the ED.

The main activities planned for 2011 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
2.1	Accounts and payments	Carrying out payments Reporting Annual accounts Postings Ledgers Inventories of assets	Accuracy, timely responses, respect of formal deadlines	Ongoing	0
2.2	Coordination of audits	Opinions of Accountant Advice to management and staff on accounting matters Coordination with external stakeholders namely, the Court of Auditors, as appropriate etc.	Number of cases supported Timely responses	Ongoing	0
2.3	Opening and Closing of the Annual Budget and preparation of Budgetary Statements.	Approved budget tree opened, appropriations posted properly.	Annual budget lines open and available by the end of the third week of the fiscal year, economic outturn account and supporting operations done on time.	By the end of January and by the end of the third week of December. Preparation by 10 December.	0
2.4	Implementation and Consolidation of Internal Procedures and Internal Controls for all financial circuits including missions.	Annual review of internal Procedures and Internal Controls. Regular carrying out of controls on all financial transactions.	Guidelines and check-lists reviewed. Annual risk assessment. Controls updated accordingly. Training sessions to create awareness of procedures and controls. Carrying out of controls.	Quarterly	0
2.5	Annual budget reports	Monthly	Budget status reporting for all areas, Titles and Department, as necessary, including analysis of main relevant aspects.	Monthly (for the previous month)	0
2.6	Organising carryovers	Support the Departments in dealing with carryovers	Communication Time and control	Annually by end of second week of the year	0
2.7	Payroll administration	Financial aspects of payroll management in co-operation with HR Payroll planning and control	Timely payment of salaries and liaising with PMO as appropriate	Monthly	0

8.3 Human Resources

Human resources carry out recruitments, performance evaluations, organisation of trainings, health and safety at work, leave management handling of individual rights and payroll management. In 2011 the scope of HR is to consolidate the organisational changes of 2009 that mark a shift towards greater hierarchical control of the Agency when delivering on its operational work program. In 2011 the priorities of the HR Section include:

- Multi annual resource planning
- Affirmative measurable measures for staff retention (attrition rates, goals, cost of turnover, trainings, promotions etc.)
- Services through electronic workflows

The main activities planned for 2010 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
3.1	Staff Policy Plan and implementing rules	Draft, update and follow-up of changes to the SR and its IR as well as to other staff guidelines as necessary. Draft, update and follow up the Staff Policy Plan	Updated implementing rules Communicate with Staff. Liaise with Staff Committee and Commission on Implementing Rules and Staff Policy Plan	Ongoing	0
3.2	Title 1 Payroll and individual rights Grading Committee	Monthly Payroll and employer duties carried out on time. Individual rights. Grading Committee.	Administer Title 1 and payroll. Control HB Postings. Coordinate with ACC and PMO on accuracy of postings. Ex post control of payments.	Monthly. Grading Committee (2-4 sessions p.a.)	4 669 500
3.3	Staff Performance Evaluation	Annual performance and probationary period evaluations. Timetables and communication. Appeals' support. Monitor job descriptions and job performance.	Number of evaluations. Planning. Timely conclusion of procedures	Once per year. For probation period, as appropriate	0
3.4	Annual Training Programme	Training Program (in-house, external, upon individual initiative). Preparation, handling and assessment of trainings.	Training planning Document presentation and acceptance. Training programmes to cover key performance areas.	Yearly	104 000
3.5	Recruitment plan	Execute the Agency recruitment plan in line with the Establishment Plan. Publish vacancy notices. Organise Selection Committees. Communicate with candidates. Induction for new recruits.	Number of Staff hired to cover new posts or make up for resignations. Speed of hiring. Planning Staff resettlement guidance.	On going	294 964

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
3.6	Health and Safety at Work	Annual Staff Health and Safety Programme	Administer Health and Safety Programme (Medical inspections, pre-recruitment medical visits, working conditions, first aid, medical adviser, medical centre).	Yearly	51 500
3.7	Third party services	Interim services and consultants	Interim services to cover up for very short assignments, tasks and seasonal support. Consultants in the area of T1, such as Legal consultancy.	Yearly	215 000

8.4 Legal

The Legal Section carries out budget implementation and control activities that include general contract management and public procurement of the Agency. The Legal Section services the Agency with regard to litigation and pre-litigation support. The Legal Section plays a role to ensure compliance with regard to prevailing legal rules and regulations and in order to make available service to management and staff as appropriate in order to meet compliance objectives. The Legal Section makes available to the Agency legal advice, legal services as well as procurement guidance and services. The Legal Section may also carry out ad hoc operational tasks as it might be needed and agreed with the operational Departments. In 2011 the priorities of the Legal Section include:

- Efficient procurement project planning and execution.
- Contract management planning
- Follow up on compliance matters

The main activities planned for 2011 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
4.1	Legal Advice, as requested by the ED and Departments. Data Protection[25] Coordination	Legal opinion as requested. Representation of the Agency in all appropriate instances. Participation in internal and external events and work. Data Protection officers' tasks and reporting to EDPS	Number of internal cases handled (legal opinions, complaints, legal cases, reports summarizing key elements and sharing relevant information) Data protection coordination	Ongoing	0
4.2	Public Procurement	Regular carrying out of public procurement procedures and appropriate assistance provided to all Departments. Procurement planning.	Procurement Plans, routing slips and forms available, number and type of procurement processes handled, files organized. Purchase Order files. Suppliers' data base. Enquiries handled. Procurement planning and consolidation of procurement activities.	Ongoing	0
4.3	Contract Management	General support on contract management	Number of contracts prepared and signed by the Agency, number of requests for support received from Departments, number of claims received regarding this matter. Routing slips.	Ongoing	0
4.4	Operational support	Provide legal input to ENISA Operational Activities as requested and agreed	Time spent on administering of and providing feedback to Operations.	*Ad hoc*, as requested and agreed	0
4.5	Representation	Representation in terms of formal events, and representation before Administrative and Budget Authorities and Courts as authorised by ED.	Number of cases handled	Ongoing	0

25 Legal, comprises of the tasks of the Data Protection Officer, that is an independent function that is supervised directly by the ED and/or the European Data Protection Supervisor as per Regulation (EC) 45/2001.

8.5 Summary of Administration Activities

ADA 1	General Administration	Budget line	Budget	Man months	New Activity
ADA 1.1	Planning administration activities and representation	N/A	N/A	1.5	NO
ADA 1.2	Advice and support	N/A	N/A	3	NO
ADA 1.3	Reporting levels on Agency's resources	N/A	N/A	2	NO
ADA 1.4	Audit follow up	N/A	N/A	2	NO
ADA 1.5	General organisational tasks (incl. Missions)	N/A	N/A	26	NO
ADA 1.6	Office services	a. Title 2, excluding Chapter 23 ICT & BL 2202 Telecoms b. 3230 Translations	a. 245 000 b. 44.957	10.9	NO
ADA 1.7	Handling requests of Staff members related to the implementation of the seat agreement (special ID cards, car registration, VAT exemption etc).	N/A	N/A	2	NO
ADA 1.8	Internal control coordination	N/A	N/A	0.5	NO
ADA 1.9	Business continuity coordination	N/A	N/A	0.1	YES
ADA 1.10	Events organisation	N/A	N/A	9.6	YES
	TOTAL	**See ADA 1.6**	**289.957**	**57.6**	

ADA 2	Accounting and Finance	Budget line	Budget	Man months	New Activity
ADA 2.1	Payments Accounts	N/A	N/A	19.2	NO
ADA 2.2	Coordination of Audits	N/A	N/A	1	NO
ADA 2.3	Opening and closing of annual budget	N/A	N/A	1	NO
ADA 2.4	Implementation and consolidation of internal controls including missions	N/A	N/A	14.2	NO
ADA 2.5	Annual budget reports	N/A	N/A	1	NO
ADA 2.6	Organising carryovers	N/A	N/A	1	NO
ADA 2.7	Payroll administration	N/A	N/A	1	NO
	TOTAL		**0**	**38.4**	

ADA 3	Human Resources	Budget line	Budget	Man months	New Activity
ADA 3.1	Staff policy plan	N/A	N/A	0.2	NO
ADA 3.2	Payroll administration & Grading	Chapter 11	4 669 500	6	NO
ADA 3.3	Performance evaluation	N/A	N/A	6	NO
ADA 3.4	Annual training programme	1320	104 000	3	NO
ADA 3.5	Recruitment plan	Chapter 12	294 964	11.6	NO
ADA 3.6	Health and safety at work	1310	51 500	1	NO
ADA 3.7	Third party services follow up	Chapter 14	215 000	1	NO
	TOTAL	**Title 1**	**5 334 964**	**28.8**	

ADA 4	Legal and procurement	Budget line	Budget	Man months	New Activity
ADA 4.1	Legal advice and representation	N/A	N/A	6.6	NO
ADA 4.2	Public procurement	N/A	N/A	9.6	NO
ADA 4.3	Contract management	N/A	N/A	1	NO
ADA 4.4	Operational support	N/A	N/A	1	NO
ADA 4.5	Representation	N/A	N/A	1	NO
	TOTAL		**0**	**19.2**	
	GRAND TOTAL		**5 624 921**	**139.2**	

MISS	Missions AD	3014	30.000		
MISS	Missions ED	3015	35.000		

APPENDIX A: OPERATIONAL BUDGET LINES (TITLE 3)

Table: Activities and corresponding Budget Lines in Draft Statement of Estimates 2011 (Preliminary Draft Budget 2011)

Draft Statement of Estimates 2011			Draft Work Programme 2011	
Budget Line	**Heading**	**Activity**	**Title**	**Amount**
3000	Permanent Stakeholders Group	SR 2	Permanent Stakeholders Group & NIS Stakeholders	90.000
3003	Management Board	SR 1	Management Board	110.000
3013	Technical Department Missions	MISS	Missions TCD, SR, PAU	368.000
3014	Administration Department Missions	MISS	Missions AD, ITSU	35.000
3015	Executive Director Office Missions	MISS	Missions ED	35.000
3200	Conferences and Joint Events	PAU 6	ENISA Brand Events	10.000
3210	Communication activities	PAU 5	Spokesman and Media Relations	44.000
3220	Web Site	PAU 3	ENISA Digital Communication	76.000
3230	Translations	ADA 1.6	Translations (managed by AD)	44.957
3240	Publications	PAU 4	Publications and Brand Materials	60.000
3300	Computer Incident Response Handling	a. WPK 1.3 b. WPK 1.4 c. WPK 1.5 d.WPK 2.4	a. Reinforcing CERTs in the Member States b. Support CERT (co)operation at European Level c. Good practice for CERTs to address NIS aspects of cybercrime d. Early warning for NIS	376.000
3320	Relation with EU Bodies and Member States	SR 3	National Contact Officers Networks	20.000
3330	Relations with the Industry and International Institutions	a. SR 4 b. PS 2 c. WPK 3.1 d. WPK 3.4	a. Stakeholder Relationship Management Platform b. Integrating NIS into Education c. Identifying and promoting economically efficient approaches to information security d. European Cyber Security Awareness Month	190.000
3510	Security Policies	a. WPK 1.1 b. WPK 1.2 c. WPK 2.2	a. Supporting Member States in implementing article 13a b. Preparing the Next Pan-European Exercise c. Interdependencies & Interconnection	440.000
3520	Security Technologies	a. WPK 2.1 b. WPK 2.3 c. WPK 3.2 d. WPK 3.3	a. Security & privacy of Future Internet technologies b. Secure architectures and technologies c. Deploying Privacy & Trust in Operational Environments d. Supporting the implementation of the ePrivacy Directive (2002/58/EC)	374.000
	Grand total - Title 3			**2.272.957**

APPENDIX B: OPERATIONAL ACTIVITIES 2011

Table: Budget expenditure split by Operational Activity

OPERATIONAL ACTIVITIES 2011	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 - ENISA as a facilitator for improving cooperation	9,0	733.974	596.000	515.565	1.845.539
WS2 - ENISA as a competence centre for securing current & future technology	8,5	688.886	390.000	469.438	1.548.324
WS3 - ENISA as a promoter or privacy & trust	6,0	467.073	304.000	321.717	1.092.790
Stakeholder Relations	3,0	252.118	300.000	164.654	716.772
Public Affairs	4,5	372.455	190.000	243.244	805.699
Missions & Representation	0,0	0	438.000	0	438.000
Project Support Activities	3,0	206.652	10.000	148.305	364.958
Management & Support activities	9,0	753.672	44.957	492.210	1.290.839
Total	**43,0**	**3.474.831**	**2.272.957**	**2.355.133**	**8.102.921**

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 2010.

Note 4 - Overheads include all costs which are indirectly involved in the implementation of WP 2010, such as salary costs of non-operational staff, rent, and running costs (e.g. Office supplies).

enisa
European Network
and Information
Security Agency

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu