enisa

European Network
and Information
Security Agency

WORK PROGRAMME 2010

Build on Synergies – Achieve Impact

www.enisa.europa.eu

Contents

1 INTRODUCTION

This Work Programme defines and describes the Multi-annual Thematic Programmes (MTPs), horizontal activities, provision of advice and assistance and administrative activities of the European Network and Information Security Agency (hereafter also referred to as the Agency) foreseen for 2010. As such the Work Programme provides the main tasks and the budget for 2010 activities of the Agency.

1.1 Relation to previous versions

This version of the work programme has been released to take account of a number of changes that have been agreed subsequent to the arrival of the new Executive Director of ENISA on 16 October 2009. These changes can be summarised as follows:

- *Organisational re-alignment of ENISA, as communicated to the Management Board on 3 November 2009.*
- *Greater prioritisation of MTP1 and increased focus on the requirements of the Commission's Communication of March 2009, COM(2009)149.*
- *Removal of the Pan-European Information Security Survey from WPK 2.1.*
- *Removal of WPK 3.3 (Application of the 'Emerging and Future Risk Framework' with Stakeholders) from MTP3.*
- *Increased focus on enhancing national risk management preparedness in order to further support the CIIP action plan (WPK 3.4).*

These changes have been made in response to requests by members of the Management Board to focus more on key activities.

1.2 Policy context

The Commission Communication "i2010 – A European Information Society for growth and employment"[1], highlighted the importance of network and information security for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and society.

The Communication "A strategy for a Secure Information Society"[2] recognises that a secure Information Society must be based on enhanced Network Information Security (NIS) and a widespread culture of security. This can only be achieved through a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment. Where stakeholders are concerned, it is important to recognise that creating a strong NIS culture is a challenge for everybody.

[1] COM(2005) 229, 01.06.2005

[2] COM(2006) 251, 31.05.2006

A Council resolution of December 2006[3] calls the Agency to support the strategy of the European Commission within its mandate as it is set out in the founding Regulation of the Agency. ENISA achieves this by aligning its strategy and annual work plans with the strategy of the European Commission. In an effort to maximise the impact of its activities, the Agency leverages existing synergies and initiatives at national and European level in a focused and impact oriented approach.

The Commission Communication of March 2009[4] entitled “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 proposed action plan to strengthen the security and resilience of CIIs. This work program responds to this call mainly within the context of MTP1, but also includes activities in MTP2 and MTP3 that support this action plan.

1.3 Key challenges

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, as an attacker will seek to exploit the weakest link in any system.

Such a response requires a structure that encourages collaborative action and enables all relevant stakeholders to work together in defining appropriate priorities and means to ensure an adequate level of NIS in the EU. The highly dynamic application environment that is continually expanding and providing new services for business and government makes his need even more pressing.

Any attempt to define and implement such an approach, must take place against the backdrop of rapidly changing technological developments, such as Radio Frequency ID (RFID), the Internet of things and the Future Internet while not ignoring other important trends and challenges such as financially motivated organised cyber-crime and politically motivated cyber-attacks.

Whilst the technical challenge of securing new technological advances remains, the number one priority concerns the set up of a proactive security culture. Creating such a culture, in turn, requires several factors to be considered, such as the multi-stakeholder environment, educational gaps, non-optimised business models, imbalance in Member States’ capabilities, approximation of laws and the global scope of network and information security issues.

1.4 ENISA’s role

ENISA, is uniquely positioned to provide advice and assistance to Member States in enhancing their network and information security capabilities. Due to its independent position, the Agency can provide well-informed, objective advice and play a significant role in supporting the Commission and Member States by facilitating the exchange of good practices and information between all stakeholders at European level, thus maximizing results and impact.

[3] 15768, 01.12.2006
[4] COM(2009) 149

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 (National Liaison Officers – NLO), 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.

The capacity to provide prompt, independent and high quality response to Requests received from EU Institutions and Member States' competent bodies gives the Agency a bridging role between EU and national institutions. This role is specific to ENISA and currently it is unique in the world.

A closer participation in the worldwide dialogue is also being developed through continuously expanding contacts with Third Countries in all Continents as well as with international institutions (e.g., ITU, IETF, OASIS, OECD). The expected impact is a better integration of important foreign player views and a promotion of European approaches.

1.5 Multi-annual planning

Due to its mandate and limited resources, the Agency has been directed by the Management Board to focus its efforts on a realistic set of strategic priorities. By concentrating its efforts, the Agency aims to achieve increased impact in key areas. In order to achieve this, the Agency will leverage existing national and EU activities avoiding duplication of effort and maximizing results. Examples of such European activities are the IST-FP6 Research for Critical Information Infrastructure Protection (CIIP), the Competitiveness and Innovation Programme (CIP), the ICT priority in the 7th Research Framework Programme and the IDABC (Interoperable Delivery of European eGovernment services to public Administrations, Business and Citizens) programme. To work closely with these initiatives, capitalise on their results, interact with their constituencies and engage them in ENISA's work is one of the key elements of this Work Programme.

To achieve the desired impact and build on synergies, the Agency follows a multi-annual work plan. One of the key objectives of this approach is to implement high-level orientations provided by the ENISA Management Board[5], while concentrating efforts on a limited set of strategic priorities, called Multi-annual Thematic Programmes (MTP). These programmes define the work of the Agency for a number of years. A set of SMART[6] goals are defined for each programme. These goals are related to the desired outcomes and impacts and can be assessed and monitored during the duration of the programme via Key Performance Indicators.

Each thematic programme consists of several Work Packages (WPK), that implement the SMART goals of the MTP. Each Work Package defines the tasks, the stakeholders concerned, the desired impact and the resources needed.

[5] These high-level goals are:

- Building confidence in the information society through increasing the level of NIS in the EU;
- Facilitating the Internal Market for e-Communication by assisting the institutions to decide the appropriate mix of regulation and other measures (noting in particular, the important contribution the Agency can make to the Framework Directive);
- Increasing the dialogue between the various stakeholders in the EU on NIS;
- Increasing co-operation between MS in order to reduce the difference in the capability of MS in this area;
- Assisting and responding to requests for assistance from the Member States.

[6] SMART is an acronym for Specific, Measurable, Agreed, Realistic and Time bound.

Work Packages may be multi-annual. However, since MTPs are implemented through the Agency's annual Work Programme, the indicated resources and budget refer to actions, outcomes and operations of a specific year. The specified budget refers to external activities e.g. workshops, conferences or consultancy. The human resources refer to the effort put by the Agency's experts.

Work Programmes may also include Preparatory Actions (PAs). A PA is an activity that is designed to complete in one year and is used to determine whether or not a new MTP should be initiated. A decision can is taken once the results are available.

In 2008, the Agency started with three MTPs and one PA. In 2009, the focus was consolidated around the existing MTPs, while integrating the follow-up of the PA as WPKs in one of the MTPs. In accordance with the conclusions of the informal MB/PSG workshop held in June 2009, the Agency will continue working on these three MTPs in 2010, while introducing two new PAs, which are briefly described here. A full description of the MTPs and PAs, as well as, the individual WPKs is given in the next chapter. The WPKs proposed for 2010 include their own SMART goals and KPIs that are considered as a first step toward achieving the corresponding SMART goals.

MTP 1: Improving resilience in European e-Communication networks

In 2008, this MTP focused on stocktaking, best practices identification and analysis of gaps of measures deployed by both National Regulatory Authorities (NRAs) and network operators and service providers. MTP 1 also analysed the suitability of currently deployed backbone internet technologies regarding integrity and stability of network. In 2009, MTP 1 compared the findings against similar international experiences and results, issued guidelines, and finally formulated consensus-based recommendations after broad consultation with concerned stakeholders. In 2010, the main effort in this area will be to support the actions described in the recent communication on CIIP released by the Commission in March 2009.

MTP 2: Developing and maintaining co-operation between Member States

In 2008 the MTP aimed at a) the identification of Europe-wide security competence circles on topics such as Awareness Raising and Incident Response, b) the European NIS good practice Brokerage[7]. In 2009, NIS capacity building for micro enterprises was added for the duration of one year. In 2010, further co-operation among Member States will be developed further and international cooperation opportunities will be explored with the aim of improving the capabilities of all Members States and increasing the overall coherence of the approach to NIS at the pan-European level. Due to its limited resources, the Agency will cooperate closely with the Commission services in order to minimize its efforts and maximize the results.

[7] This platform is a follow-up of the work conducted in 2007 to define a roadmap on the establishment of European NIS good practice Brokerage.

MTP 3: Identifying emerging risks for creating trust and confidence

The Agency has established a framework that will enable decision makers to better understand and assess emerging risks arising from new technologies and new applications. One of the principal goals of this framework is to help stakeholders' develop mutual trust and confidence in dealing with emerging risks. To this end, the Agency developed a proof of concept in 2008 of a European capacity for the evaluation of risks that may emerge in 2 to 3 years ahead, linked to a Stakeholder Forum for multi-stakeholder dialogue with public and private sector decision makers. In 2009, this proof of concept was tested and developed further with the aim to deploy it with Member States in 2010. The Agency will continue preparing Risk Assessment reports to express the Agency's view on emerging risks arising from new technologies and new applications. In addition, the Agency will explore topics related to accountability and trust in the future Internet. As such, this MTP should provide an antenna function for decision makers in Europe and possibly beyond.

PA1: Identity, accountability and trust in the future Internet

Following recent developments of the Internet, in parallel to their real life, each person has the opportunity of living additional lives in the virtual world. A trend observed over the last few years, first in the research community, but now also in commercial offerings is the increase of interactions between these two worlds, making real-world information accessible to services on the Internet. A parallel development is the so-called Internet of Things (IoT) which, as an evolution of today's RFID technology, consists of networks of actuators and sensor nodes that interact with objects bearing tags. As a response to these developments, the overall goal of this Preparatory Action is to "ensure that Europe maintains a high level of security and confidence of both users and industry on the ICT infrastructure and provided services, while at the same time limiting the threats to civil liberties and privacy".

PA2: Identifying drivers and frameworks for EU sectoral NIS Cooperation

As intangible assets have become increasingly core to companies' value, general economic and operational incentives for the development of public-private cooperation in tackling NIS challenges are increasingly required. Traditional forms of protection are no longer enough to prevent intruders from entering and stealing or damaging key assets and a more proactive approach is needed. This approach should encompass an overall framework of organisational differentiation between public and private actors and along organisational supply chains, based on a realistic assessment of various parties' ability to tackle NIS challenges, taking into account their legitimate commercial or public service responsibilities and capabilities.
The purpose of this PA is to clarify the question of how to get commitments from relevant actors to collective action to address NIS challenges at a pan-European level.

In addition to the above, the Agency will continue performing a number of horizontal activities, such as communication and outreach, secretariat of ENISA bodies, relations with external stakeholders (EU Bodies, Member States, industry, academia, consumers, International Institutions and Third Countries), the Agency's internal capabilities, internal communication and Work Programme development.

Also, the Agency will continue providing advice and assistance when called upon. Finally, the Agency's Administrative Department implements general administration, finance, human resources, ICT and legal and procurement. With regard to career development, the Agency has at its disposal a finite number of instruments that includes grading, promotions, trainings and career opportunities within the Agency.

2 MULTI-ANNUAL THEMATIC PROGRAMMES

2.1 MTP 1: Improving resilience in European e-Communication networks

THEME NAME :

MTP 1: Improving resilience in European e-Communication Networks

DESCRIPTION OF THE PROBLEM TO SOLVE :

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 into other infrastructures and have a European-wide impact.

The international nature of telecommunications networks requires a common approach to deal with issues such as resilience and security. Several Member States have already developed, or are in the process of developing, strategies, policies and regulatory initiatives to cope with these issues. 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 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.

The recent European Commission's communication, COM(2009)149 recognises the importance of critical communication networks and asks ENISA to play an active role in ensuring that they are adequately protected. The communication proposes 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.

For each of these activities, strong engagement with the private and public sectors is considered to be a key success factor. Existing activities will be leveraged wherever possible.

DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

The goal of this MTP is to support the Member States and the Commission in their efforts to improve resilience by "collectively evaluating and improving security and resilience in mobile and fixed public eCommunications networks and Services in Europe".
In 2008 ENISA performed a series of stock taking exercises of regulatory and policy environments, of providers' measures, and of existing technologies and standards.
In 2009 ENISA analysed the findings of the stock taking exercises, identified the gaps between the current situation and the target situation and worked together with stakeholders (e.g. workshops, working groups of experts), to propose good current practices aimed at bridging the identified gaps.

The goal of this MTP is to support the Member States and the Commission in their efforts to improve resilience by "collectively evaluating and improving security and resilience in mobile and fixed public eCommunications networks and Services in Europe".
In 2008 ENISA performed a series of stock taking exercises of regulatory and policy environments, of providers' measures, and of existing technologies and standards.
In 2009 ENISA analysed the findings of the stock taking exercises, identified the gaps between the current situation and the target situation and worked together with stakeholders (e.g. workshops, working groups of experts), to propose good current practices aimed at bridging the identified gaps.

In 2010 ENISA intends to:

1) Support stakeholders' efforts to deploy ENISA's information sharing and incident reporting good practice guides. The Agency will work together with targeted stakeholders to enhance their understanding of existing good practice guides and recommendations. This will involve debating findings and validating them through workshops and thematic work groups and providing support for the adoption of recommendations.
2) Assist providers in enhancing the resilience of their networks. This will involve analysing legal and policy barriers to information sharing, identifying suitable resilience metrics and providing policy recommendations in the area of Botnets.
3) Further the work carried out to date in the area of secure protocols, notably DNSSEC.
4) Together with experienced stakeholders in the field, develop a holistic framework for defining, running and assessing national, and in the long term cross-border or pan European exercises. The framework will be accompanied by a number of scenarios for conducting exercises. The framework will, among other things, build on the experiences of various stakeholders, and also aims at reinforcing the role of national /governmental CERTs in planning and executing these exercises.

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

SMART goal: By 2010, the Commission will have made use of ENISA recommendations in their policy making process.	**KPIs:** Commission (yes/no),
SMART goal: By 2012, at least 2 Member States participate in an exercise pilot using the framework.	**KPIs:** # of Member States
SMART goal: By 2010, at least 50% of Member States participate in the pan European forum?	**KPIs:** % of Member States
SMART goal: By 2012, at least 50% of Member States contributed to the framework.	**KPIs:** % of Member States, # of contributions

WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

Building confidence in the information society through increasing the level of NIS in the EU
Facilitating the Internal Market for e-Communication by assisting the institutions to decide the appropriate mix of regulation and other measures (noting in particular, the important contribution the Agency can make to the Framework Directive).
Increasing the dialogue between the various stakeholders in the EU on NIS
Increasing co-operation between MS in order to reduce the difference in the capability of MS in this area

STAKEHOLDERS + BENEFICIARIES

National Regulatory Authorities, Member States Governments and EU Policy and Decision Makers, national / governmental CERTs, Public eCommunications networks and services providers (fixed, mobile and IP-based), Internet Service Providers (ISPs), Associations of Providers (ECTA, ETNO, GSM Europe), Internet Exchange (Euro IXs), Audit Associations (ISACA), Suppliers of Network Components, Systems and Software (EICTA)

WHY ENISA?

Massive cyber-attacks or other major disruptions 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.

2.1.1 WPK 1.1- Underpin stakeholders' efforts to deploy ENISA's information sharing and incident reporting good practice guides

MTP Name

Improving resilience in European e-Communication networks

WORK PACKAGE NAME :

WPK 1.1: Underpin stakeholders' efforts to deploy ENISA's information sharing and incident reporting good practice guides

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

SMART goal: at least 10 Member States participate in the discussions on Information Sharing exchange deployment	**KPI:** # of Member States
SMART goal: at least 10 Member States participate in the discussions regarding the development of harmonised incident reporting mechanisms	**KPI:** # of Member States
SMART goal: at least 10 providers, small and big, participate in the discussions regarding the development of harmonised incident reporting mechanisms	**KPI:** # of providers

DESCRIPTION OF TASKS:

In 2008 ENISA performed a series of stock taking exercises on national regulatory and policy issues related to resilience and security of their networks. Based on these findings the Agency, in co-operation with numerous public and private stakeholders, developed in 2009 good practice guides on Network Security Information Exchange (NSIE) and Incident Reporting Mechanisms. These good practice guides are the result of cooperative work with a wide range of relevant stakeholders, who extensively discussed and validated ENISA's guides though thematic workshop(s) and an open consultation process.

The main objective of this work package is to identify incentives that will encourage public and private stakeholders to deploy good practice guides identified by ENISA and its stakeholders and to work with them to enhance their understanding of the essential recommendations. The Agency will promote past results, debate with relevant stakeholders on findings, validate them through targeted workshops and thematic working groups, and empower stakeholders in their efforts to adopt recommendations.

In the area of information sharing, the Agency aims to 1) increase the number of countries establishing and running an NSIE in Europe 2) support the development of the European Forum for Information sharing between Member States (as referenced by COM(2009)149), which would be the first pan European NSIE in Europe. In that respect, ENISA will promote good practice guides to all Member States through targeted workshop(s). The Agency will foster a dialogue among experts, mobilise relevant public and private stakeholders, ensure their participation in the process, validate findings and provide assistance to Member States in the form of training to establish and run an information sharing platform.

In parallel, ENISA will bring together major NSIEs in Europe and relevant national and pan European projects to debate the possibility of developing the first pan European platform. ENISA's proposed activities on Network Security Information Exchange will feed into the on-going discussions initiated by the European Commission on the establishment of an European Public Private Partnership for Resilience (EP3R) as proposed in the Commission's CIIP action plan - COM(2009)149

In the area of incident reporting mechanisms, ENISA will identify the relevant stakeholders, both public and private, and work together with them to foster an open dialogue. This is in line with the provisions of the new 'Common regulatory framework for electronic communications networks and services' related to integrity and availability of public communication networks (e.g. article 13a of the Framework Directive 2002/21/EC).

ENISA, through structured dialogue with relevant public and private stakeholders, will develop concrete and realistic guidelines on the possible implementation of these provisions (e.g. of a breach of security or loss of integrity or annual consolidated list of incidents). The Agency will intensively and widely validate its recommendations and ensure wide acceptance of them. The implementation of good practice guides promoted by ENISA at early stages of the Telecoms Regulatory Package will encourage the harmonisation of processes and policies at national and pan European level.

ENISA will continue to work together with all relevant public and private stakeholders on the development of appropriate measures and policies that could enhance the integrity of supplies of networks and services.

OUTCOMES AND DEADLINES:

Thematic workshop and Training on Network Security Information Exchanges (Q2, Q3 2010)
Status Report on Network Security Information Exchange in Europe (Q4 2010)
Two Thematic Workshops on Incident Reporting Mechanisms (Q1, Q3 2010)
Draft Guidelines on Implementing Notification of Major Incidents (Q4 2010)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Potential stakeholders include NRAs, national policy authorities dealing with resilience of public communication networks and services, sector associations (EICTA, ETNO, EUROISPA, GSM Europe, ISACA, Euro-IX), telecom operators (fixed, mobile and IP-based), Internet Service Providers (ISPs).

RESOURCES FOR 2010 (person months and budget)

- 100,000 Euros
- 11,5 Person Months

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3a), c), d), f), and k)

2.1.2 WPK 1.2 – Assist providers in enhancing the resilience of their networks

MTP Name

Improving resilience in European e-Communication networks

WORK PACKAGE NAME :

WPK 1.2: Assist providers in enhancing the resilience of their networks

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

SMART goal: at least 10 Member States and 10 major Private Stakeholders participate in the discussions on Legal and Policy Barriers	**KPI:** # of Member States, # of Providers
SMART goal: at least 10 Member States and 10 major Private Stakeholders participate in the discussions on Metrics and Measurement Techniques	**KPI:** # of Member States, # of Providers
SMART goal: at least 10Member States and 10 major ISPs/IXs participate in the discussions on Metrics and Measurement Techniques	**KPI:** # of Member States, # of Providers

DESCRIPTION OF TASKS:

In 2008 ENISA carried out a stock taking exercise on providers' measures related to the resilience and security of their networks and developed in 2009 a number of recommendations and good practices on a number of issues. Issues include legal and policy barriers prohibiting providers' from sharing information on sensitive matters, effective means to measure resilience and security of providers, and effective policies on combating botnets.

Legal and policy obstacles significantly hamper the ability of private operators to exchange information with the relevant stakeholders. It remains unclear how existing laws or policies governing issues such as personal privacy and data protection apply to information networks or how confidentiality obligation apply to public private partnerships in the Critical Information Infrastructure Protection (CIIP) field. The majority of these laws were adopted prior to the emergence of the information society and the dependence on information networks. There remains a lack of a clear framework for effective and timely exchange of information on critical infrastructure protection including responsible and timely disclosure of vulnerabilities. This activity will seek to identify these gaps in laws and policy in order to assess how they impact the effective deployment of information exchange in the field of critical information infrastructure protection.

Though there is a proliferation of policies, measures and methodologies covering the whole life-cycle of security and resilience incidents, there are no adequate means to measure the resilience and security of networks. Significant work has been done in metrics and measurement techniques related to the availability and integrity of particular networks including SLAs. Most of them do not address the problem holistically and from a policy perspective. It is still the case that policy makers and regulators do not have a clear mechanism for measuring the resilience and security of public communications networks as witnessed by the lack of reliable metrics. ENISA aims to bring all the relevant stakeholders together (industry, academia, policy makers, international organisations, standardisation bodies) to analyse this area, to identify the current trends and relevant projects (e.g. EU funded project **AMBER**) and to work with these stakeholders to define appropriate techniques for measurement and accompanying metrics in the field of resilience. Furthermore, in the long term ENISA will seek to establish a number of national and eventually pan European Key Performance Indicators that would measure the resilience and security of our public communications networks.

Botnets are identified as major threat to internet and consequently to our critical communication services. Their proliferation and penetration is extremely high in personal computers. ENISA will study the phenomenon of botnets, take stock at national level of policies related to botnets, work together with relevant stakeholders (ISPs, IXs, EuroISPA, EuroIXs, ETNO, etc.) on a number of policy recommendations, and develop concrete suggestions on sound and implementable measurement techniques. ENISA aims at openly consulting with all relevant stakeholders on possible co-operation issues at pan European level (e.g. mutual aid assistance, information sharing, etc.).

OUTCOMES AND DEADLINES:

Legal and Policy Barriers to Sharing Sensitive Information in the context of CIIP (Q3 2010)
State of the art analysis of metrics and measurements techniques (Q4 2010)
Botnets: Policy Recommendations (Q4 2010)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

NRAs, national policy authorities dealing with resilience of public communication networks and services, sector associations (EICTA, ETNO, EUROISPA, GSM Europe, ISACA, Euro-IX), telecom operators (fixed, mobile and IP-based), Internet Service Providers (ISPs)
RESOURCES FOR 2010 (person months and budget)

- 150,000 Euros
- 13,5 Person Months

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3a), c), d), f), and k)

2.1.3 WPK 1.3 – Investigation of innovative actions

MTP Name

Improving resilience in European e-Communication networks

WORK PACKAGE NAME :

WPK 1.3: Investigation of innovative actions

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

SMART goal: At least 10 sector actors participating in the pilot applying the recommendations /guides issued for DNSSEC deployment.	**KPI:** # Sector Actors
SMART goal: Coverage of at least 200 M users by operators surveyed in the impact assessment of routing protocols	**KPI:** # Users
SMART goal: At least 10 sector actors validating the report on architectural design principles that result in true end-to-end (e2e) security	**KPI:** # Sector actors
SMART goal: Organisation of a workshop "Open Doors to Technologies Enhancing Network Resilience" for the scientific officers of the European Commission with participants from all stakeholder sectors (Vendors, Operators, Regulators, End users, etc.). At least 30 attendees and 3 different sectors represented.	**KPI:** # Attendees # Sectors Participating

DESCRIPTION OF THE WORK PACKAGE

In 2008 and 2009 ENISA has analysed a number of technologies, protocols and architectures (namely IPv6, Multiprotocol Label Switching and DNS Security Extensions) in terms of their potential to improve the resilience of public communications networks. In this context, incentives (on market and/or policy related aspects) were considered with a view on their impact on business practices. Recommendations and good practices guides were developed mainly addressed to EU and national policy makers. Not limiting itself to technologies, architectures and protocols the Agency has also assessed the impact of networking technologies trends (e.g. cloud computing, sensor networks, online detection and diagnosis systems, etc.) on security and availability of networking resources and has drawn directions for future research. Those tasks were carried in close collaboration with two Experts Groups composed of actors from all relevant sectors. Based on the experience of 2009, the Agency will continue building upon these two groups of experts.

During 2009, ENISA developed good practices guides for deploying DNSSEC. They presented the main considerations that have to be made by providers deploying the technology and the items that should be included in policy and practices statements for Trust Anchor Repositories. The main objectives of this work package are to test or deploy the recommendations in real working environments, aiming to receive feedback on their effectiveness, validity and appropriateness. ENISA intends to widely promote such recommendations, mainly addressed to EU and national policy makers, in an effort to support the fastest take-up of most promising innovative actions. Also, the experience working in this area will create input for the Awareness Raising Section of the Agency in preparing an information campaign targeting users or specific user groups on the risks of DNS and DNSSEC in casual web-browsing applications such as banking, shopping, etc.

Securing the DNS is an act in the process of achieving a high level of resilience and security in public communications networks. Another crucial infrastructure in the public eCommunication networks, that needs to be resilient, is the routing infrastructure. In this respect, ENISA aims to assess the impact of deploying resilient routing technologies. The assessment will be used to produce guidelines/recommendations for their deployment, targeting policy makers.

In parallel to those activities, ENISA will extend its work on assessing the impact of networking trends to the resilience of public communications networks by identifying and promoting architectural design principles that result in true end-to-end (e2e) security. Initially the focus in this area was on the technologies of the transport layer of communications networks. However, public communications networks constitute the basis upon which a plethora of applications/service is offered via service providers that in many cases are independent from the network operator. In this respect, what is of interest to users of ICT services is e2e resilience and security and not only a resilient and secure transport network. Rather than aiming at identifying performant architectures it is more appropriate to identify the design principles. Individual architectures may be strongly bound to the particularities of the technologies they deploy, whereas the principles are likely to remain the same across technological boundaries.

Finally, those activities will also be combined with a targeted workshop entitled "Open Doors to Technologies Enhancing Network Resilience". The aim of this activity, is to provide to the Scientific Officers of the European Commission (DG INFSO, DG ENTR, JLS, MARKT and Research) an insight on the subject of communication networks resilience and the activities of ENISA in this area. Following the experience gathered during 2009, this activity could be expanded beyond the scope of WPK1.3 (technologies) to cover all aspects of MTP 1 (including policies).

OUTCOMES AND DEADLINES:

Preparatory plan for information campaign targeting users or specific user groups on the risks of DNS and DNSSEC in casual web-browsing applications such as banking, shopping, etc. (Q3 2010).
Report on the pilot(s) promoting the work of WPK1.3 of 2008-2009 on "improving the resilience of DNS" (Q4 2010).
Assessment of the impact of the deployment of resiliency enabled routing technologies and development of guidelines/recommendations (Q4 2010)
Report on architectural design principles that result in true end-to-end (e2e) resilient and secure public communications networks (Q4 2010).
"Open Doors to Technologies Enhancing Network Resilience" workshop (Q4 2010).

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Networking equipment vendors, National Regulatory Agencies (NRAs), Network operators, Virtual network operators, Experts in resilient backbone and internet technologies, Industrial R&D institutions, Universities and Research centres, European Technology Platforms (e.g. eMobility, NEM, NESSI, etc.).

RESOURCES FOR 2009 (person months and budget)

- € 195.000 (workshops, consultancies, running of the experts groups, electronic and printed publications).
- 17,5 person months

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3a), b), c), f), and k)

2.1.4 WPK 1.4 – Empower stakeholders towards the first pan-European exercise

MTP Name

Improving resilience in European e-Communication networks

WORK PACKAGE NAME :

WPK 1.4: Empower stakeholders towards the first pan European exercise

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

SMART goal: At least 50% of Member States participate in the discussions on the first pan European exercise	**KPI:** % of Member States
SMART goal: At least 3 Member States deploy ENISA's good practice guide on exercises	**KPI:** # exercises
SMART goal: At least 30% of Member States express their support in ENISA's framework for conducting exercises	**KPI:** % of Member States

DESCRIPTION OF TASKS:

ENISA's good practice guide on national exercises reveals the importance of exercises in checking adherence of public and private stakeholders to specified emergency preparedness measures. The recent CIIP Communication highlights the importance of exercises in improving emergency preparedness measures. Until now only a small number of Member States have deployed exercises to test their preparedness measures.

In the context of this work package, ENISA aims to facilitate the dialogue at pan European level on exercises. The Agency will assist Member States in bringing together stakeholders that could work together towards the design, development, implementation and assessment of the first pan European exercise. In order to achieve this, ENISA will work closely with The Commission and the Member States to ensure a close collaboration with all relevant stakeholders and pan European projects (e.g. EPCIP funded projects).

This will involve working together with key stakeholders to enhance their understanding on good practice guides on national exercises validating the contents through targeted discussions and thematic working groups, and finally assisting them in their efforts to participate in the first pan European exercise.

Through this dialogue ENISA will try to develop a number of possible scenarios to be used for conducting the first pan European exercises (e.g. identification of critical paths) and propose a holistic framework for conducting exercises at national, cross-border or even pan European level. The framework, together with the possible scenarios, will enable public and private stakeholders to define, organise and run preparedness exercises. Possible building blocks of the framework include stakeholders' profiles (target audiences and organisers), type of exercises, preparedness measures to be tested, possible scenarios, assessment methodologies, etc. ENISA will validate the proposed framework and the possible scenarios through a thematic workshop and interaction with experts.

Within this context, ENISA will continue collaborating with activities and projects related to emergency preparedness issues. The Agency will collaborate with an EPCIP funded study that evaluates how well emergency preparedness is achieved in Europe and assesses possible future policies, measures and guidance that would improve the level of preparedness and co-operation within the Telecommunication sector on a European scale. Also ENISA will continue working with EU Commission and Member States on implementing the actions of (COM 2008 130) "Reinforcing the Union's Disaster Response capacity". ENISA, in co-operation with relevant stakeholders, will facilitate a dialogue on improving co-operation, information sharing and mutual assistance among stakeholders during disaster response in telecommunication sector. Based on the findings and results of these actions, ENISA will seek the advice of its stakeholders on the next possible steps in the area of emergency preparedness and disaster recovery. Based on this input ENISA will formulate a number of policy recommendations for additional work on emergency preparedness and disaster recovery.

OUTCOMES AND DEADLINES:

Thematic Workshop(s) on exercise framework (Q2 2010)
Framework for conducting Exercises (Q4 2010)
Policy Recommendations on Emergency Preparedness and Disaster Recovery

STAKEHOLDERS

NRAs, national policy authorities dealing with resilience of public communication networks and services, sector associations (EICTA, ETNO, EUROISPA, GSM Europe, ISACA, Euro-IX), telecom operators (fixed, mobile and IP-based), Internet Service Providers (ISPs), European Commission, CERT communities

RESOURCES FOR 2010 (person months and budget)

- 100,000 Euros
- 13,5 Person Months

WORK PACKAGE PROPOSED BY:

ENISA, Management Board, COM

LEGAL BASE

ENISA Regulation, articles 3a), c), d), f), and k)

2.2 MTP 2: Developing and maintaining co-operation models

THEME NAME :

MTP 2: Developing and maintaining co-operation models

DESCRIPTION OF THE PROBLEM TO SOLVE :

Many Member States have the need to increase their capabilities in various fields of network and information security (NIS). Several Member States already cooperate by sharing information on best practices, but this does not happen on a structural basis. This implies missed opportunities to create synergies and improve efficiency and effectiveness at European level.

DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

By this MTP, ENISA will address these needs by fostering its role as facilitator, centre of expertise and advice broker. ENISA technically competent experts will develop various co-operation models in pre-defined areas (awareness raising, incident response and NIS capacity building for micro enterprises), while building on previous work. In addition, the Agency will further develop the European NIS Good Practice Brokerage, including supporting tools such as the Online Platform to support the dialogue, Who-is-Who Directory, Country Pages and Country Reports of the activities in the Member States. A highlight will be the various thematic workshops that will foster the relation to existing NIS communities (e.g., CERTs) or build up new communities that share common interests in specific NIS topics (e.g., Awareness Raising). The Agency will leverage on its existing contacts and networks, including the National Liaison Officers network and identified National Competent Bodies.

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

SMART goal: By 2010, at least 10 Member States have participated in at least 3 different co-operation models.

KPIs: # Member States involved,
# Co-operation models

WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

Building confidence in the information age by increasing the capabilities of the Member States in the field of NIS.
Increasing co-operation between MS in order to reduce the difference in the capability of MS in this area.
Increasing the dialogue between the various stakeholders in Europe on NIS

STAKEHOLDERS + BENEFICIARIES

MS governments (and NRAs); Commission; industry; academia; other stakeholder groups.

WHY ENISA?

ENISA is uniquely positioned to provide advice and assistance to Member States and the Commission in enhancing their network and information security capabilities. ENISA provides an independent European-wide platform to facilitate co-operation between Member States, acting as trusted third party. ENISA has already performed valuable work in awareness raising, CSIRTs, feasibility study on an EU-wide information sharing and alert system, brokering between Member States and micro enterprises.

PROGRAMME PROPOSED BY:

ENISA, Management Board, Permanent Stakeholders' Group

LEGAL BASE

ENISA Regulation, articles 3c), d), and e)

2.2.1 WPK 2.1- Co-operation platform for Awareness Raising (AR) Community

MTP Name

Developing and maintaining co-operation models

WORK PACKAGE NAME :

WPK2.1: Co-operation platform for Awareness Raising (AR) Community

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

SMART goal: By 4Q 2010, have at least five white papers compiled with the support of the AR Community. Topics will be identified taking into consideration the composition of the AR Community (e.g. members' interests) and research/survey conducted by the Agency.	**KPIs:** # white papers.
SMART goal: By Q2 2010, organise a conference with at least 100 participants from at least 10 EU Member States.	**KPI:** # participants, # EU Member States represented.

DESCRIPTION OF THE WORK PACKAGE

This work package intends to further develop and strengthen the AR Community and maintain it as a valuable co-operation platform for raising security awareness and promoting best practices in NIS throughout the EU. It is also the intention to involve the AR Community in supporting ENISA in its mission to foster a culture of information security.

To this end, three main activities have been identified as enablers to achieve these goals: AR Community and AR Conference.

AR Community

ENISA will further develop and strengthen the AR Community after two year of rapid growth. The Agency will facilitate discussions, exchange of good practices and knowledge sharing by different means of communications during which cutting-edge topics, key issues and emerging awareness good practices will be discussed and presented. The members of the AR Community will be requested to engage with the Awareness Raising Section of ENISA in its mission to foster a culture of information security. Members will be a point of contact for matters related to information security awareness in general or related to their countries, industries, or areas of activity. They will contribute e.g., by participating in discussions and drafting White Papers on specific security topics, including awareness raising for SMEs, taking part to virtual working groups building-up to the present work. Relevant material will be made available on the AR Community portal (e.g. reports; training material; factsheets etc.).

AR conference

In 2Q 2010, ENISA will organise a conference to present current best practices in the field of Awareness Raising. Topics will be selected on the basis of the findings of ENISA and the AR Community in the field of information security awareness.

OUTCOMES AND DEADLINES:

AR conference aimed at reporting on good practices material and recommendations to enhance co-operation among Member States (2Q 2010)

Internal contact list of awareness raising experts part of the ENISA AR community (ongoing task; 4Q 2010)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Member States, PSG, Industry Associations, AR Community

RESOURCES FOR 2010 (person months and budget)

- 24 person months
- € 60.000

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3c), d) and e)

2.2.2 WPK 2.2- Security competence circle and good practice sharing for CERT communities

MTP Name

Developing and maintaining co-operation models

WORK PACKAGE NAME :

WPK 2.2: Security competence circle and good practice sharing for CERT communities

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

SMART goal: By Q4 2010, at least 10 references to ENISA good practice material "CERT services" from external websites, official publications, discussions on mailing lists or other means.	**KPI:** # of references
SMART goal: By Q4 2010, at least 10 references to ENISA reference material for supporting pan-European cooperation among national / governmental CERTs 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 CERT workshop	**KPI:** % of EU population represented
SMART goal: Workshop participants score the CERT workshop at least as 3 on a scale of 1-5	**KPI:** Average feedback on scale of 1-5
SMART goal: By Q4 2010, at least 3 presentations given about ENISA's work in the CERT field at the CERT/CSIRT community events.	**KPI:** # of presentations
SMART goal: By Q4 2010, 80% of updates in CERT inventory are confirmed	**KPI:** % confirmed updates
SMART goal: By Q4 2010 at least two TRANSITS trainings have been organised with support by ENISA[8]	**KPI:** # of trainings supported

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

DESCRIPTION OF TASKS:

ENISA's work in the field of CERT cooperation and support has reached a crucial point: almost all EU Member States have at least one response team in place that is able to act as an interims point of contact for incident management and reporting, or have initiated projects that will lead to its establishment. However some Member States have not yet in place an official national / governmental CERT with an official mandate to carry out services for the protection of national information infrastructure and to cooperate with national / governmental CERTs in other Member States. Therefore ENISA will focus this year's work on further facilitating the setting up, training and exercising of national / governmental CERT capabilities and their cooperation on European level. A special emphasis will be laid on fostering the cooperation among national / governmental CERTs, by discussing with the stakeholders and agreeing on the capabilities, requirements, needs, obstacles and other issues to enable all Member States to involve in information sharing activities on incidents, vulnerabilities and other topics in relation to CIIP.

Good practice in providing CERT services

Based on the survey from 2009 that resulted in a list of "baseline capabilities for national / governmental CERTs in Europe" a more in-depth analysis of good practice in providing these services. ENISA will create a good practice guide for a specific service that the list highlighted as important, and that is not yet covered by a good practice collection. Very promising services may be the following:

- Watching and Early Warning (and related topics like anomaly detection, correlation of events, sensor networks, etc.)
- Vulnerability research and disclosure
- Malware analysis (and related topics like honeypots and –nets, malware-db, etc.)

Facilitate cooperation and information sharing

Cooperation and information sharing for national / governmental CERTs on European level is of crucial importance for a pan-European approach towards incident management. ENISA will investigate how to assist the community to facilitate cooperation and information sharing further. The starting point will be a reference document for supporting pan-european cooperation among national / governmental CERTs, based on the report "CERT cooperation and its further facilitation by relevant stakeholders" from 2006. The report will be updated, with a special emphasis on the organisational needs of Member States in relation to information sharing. Experiences with constructs like the European Government CERT Group (EGC) and sector-based ISACs will go into this document. The document will also provide ENISA with an insight in crucial next steps to prepare for the coming years. The creation of this new document will be accompanied and discussed with the relevant stakeholders in appropriate ways like ad-hoc working groups, presentations at CERT meetings, etc.

Reinforce Member States capabilities – EISAS follow-up

In 2006/2007 ENISA carried out a study in order to assess the "Feasibility for a Europe-wide Information Sharing and Alerting System" (EISAS), targeted at SMEs and citizens. Two complementary pilot projects for implementing the findings of this study are carried in 2009/2010, financially supported by the European Commission. The European Commission in its Communication COM(2009(149)) asked ENISA to take stock of the results of these two projects and other national initiatives end of 2010, and to produce a roadmap to further the development and deployment. In 2009 ENISA started to follow the process in these two projects and will, depending on the availability of the project leaders, continue to monitor progress in 2010. ENISA targets at preparing the draft roadmap end of 2010, taking into account the results of the projects and other (national) initiatives. The roadmap should point out the way forward for further development in the area of information sharing for citizens and SMEs.

5th 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 5th edition of the workshop “CERTs in Europe” will focus on “the role of national / governmental CERTs in national and international exercises” and will aim at sharing information on good methodological and organisational practice for national / governmental CERTs that are involved in running of exercises for CIIP in their Member State. Furthermore this workshop will touch the topic of participation in international exercises like ASEAN drill, Cyberstorm, etc. The outcome of this workshop will be used to assess further steps ENISA can take with the relevant stakeholders in order to reinforce the capabilities of national / governmental CERTs for national and international exercises, and the results will be used to facilitate the outlining of the exercise framework, described in WPK 1.4 under MTP1 “Resilience”.

Continue facilitation of the setting up of CERTs/CSIRTs and stay in close relation to the various CERT/CSIRT communities

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. MS 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. The ENISA CERT Inventory will be updated to reflect the developments in the European landscape accordingly.

Present and represent

ENISA will furthermore continue to strengthen its position as independent and experienced contact for the various European and International CERT communities like TF-CSIRT and FIRST. This will be accomplished by presenting ENISAs work in events organised by these communities, and enable the communities to influence the agencies work by giving feedback.

OUTCOMES AND DEADLINES:

- ENISA good practice guide on providing of a CERT service in Q4
- ENISA reference document on pan-European cooperation among national / governmental CERTs in Q4
- Draft roadmap “EISAS” in Q4 2010
- 5th Workshop CERTs in Europe (Q2)
- Updated “ENISA Inventory of CERTs in Europe” in Q2 and Q4 2009
- At least 2 TRANSITS courses supported by Q4

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

EU Member States (in particular national CSIRTs), European Commission, CERT community

RESOURCES FOR 2009 (person months and budget)

- € 135.000 (workshop, meetings, consultancy, facilitation of exercise, support of TRANSITS courses)
- 24 person months

WORK PACKAGE PROPOSED BY:

ENISA, European Commission

LEGAL BASE

ENISA Regulation, articles 3c), d), and e)

2.2.3 WPK 2.3- European NIS good practice Brokerage

MTP

Developing and maintaining co-operation models

WORK PACKAGE NAME :

WPK 2.3: European NIS good practice Brokerage

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

SMART goal: By Q3 2010, publication of Country Reports and Who-is-Who covering relevant NIS policies, governance practices and contacts in CII resilience, e-identity and personal data breach notification in all the Member States (including EEA and EFTA countries).	**KPI:** # good practices identified in CII resilience, e-identity and breach notification.
SMART goal: By Q4 2010, good practice brokerage projects launched in CII resilience, e-identity and breach notification for countries in critical need, as identified in the Country Reports.	**KPI:** # stakeholders and # countries involved in projects on CII resilience, e-identity and breach notification vis-à-vis needs identified in Country Reports.

DESCRIPTION OF TASKS:

Since 2007, ENISA has been facilitating cooperative projects among EU Member States through its European NIS Good Practice Brokerage.

Previous brokerage activities included the following:

- In the field of CERT, ENISA facilitated cooperation projects between Hungary and Bulgaria to establish the Bulgarian Governmental CERT, and between CERT-FI (Finland) and CSIR/MERAKA (South Africa) to exchange of good practices and establish a South African CSIRT.
- In the financial sector, ENISA facilitated development of a public-private partnership for the structured exchange of cyber-crime related information between the financial sector and governments by means of Financial Information and Analysis Centers (FI-ISAC), involving more than 15 countries and relevant private sector stakeholders.

- In the field of awareness raising, ENISA in 2009 facilitated a Scandinavian Local Governments meeting on Information Security aimed at the developing exchanges of good practices concerning the management of information security within municipalities and regions in Denmark, Sweden, and Norway.
- In the field of resilience and CERT, ENISA expects to facilitate a cooperation project among Malta and another country (if not a number of countries) towards the end of 2009 or the start of 2010.

In order to enhance the overall level of NIS in Europe, much improved cooperation among both Member States and the private sector is essential. The 2009 European Commission Communication on Critical Information Infrastructure Protection (CIIP) "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" calls for a new European multi-stakeholder governance model fostering "the involvement of the private sector in the definition of strategic public policy objectives [...]" (cf. Chapter 3.4.2). Building on its initial success with the financial sector, ENISA will continue to develop its brokerage with not only Member States (including EEA countries) and Third countries, but also with major public and private sector organisations. This will enable:

1. Transfer of good practices between countries with already-developed structures and those without;
2. Identification and development of new governance practices required by newly emerging threats by some if not all countries.

In 2010, the Brokerage Work Package will be more deeply integrated with work being done in MTP1 and PA1.Cooperative projects will thus focus in particular on developing the exchange of good practices in resilient, sustainable and secure infrastructure and services, enhancement of national/governmental Computer Emergency Response Team (CERTs) and the development of public-private cooperation fora such as EISAS and the FI-ISAC, and e-identity, authentication, data protection, privacy and trust issues, with the aim of identifying key measures for maintaining a high level of security and confidence in a number of economically vital but fast-changing sectors for Member States.

With a view to identifying good practices and potential partners in cooperation projects in these crucial areas, while building on expertise already developed, the Agency will re-focus the existing Country Reports on policies and governance practices for CII resilience, e-identity, authentication, and the management of personal data (particularly breach notification). The Reports will thus provide an inventory of existing NIS good practices, and will be complemented by a similarly re-focused Who-is-Who Directory identifying relevant stakeholders (both public and private) in these areas.

The NIS good practice Brokerage will be supported by an online platform (an extranet for relevant stakeholders that ENISA expects to develop from September 2009) with information about completed and on-going co-operation projects, an inventory of NIS good practices, and the online publication of the Country Reports and Who's Who Directory. The online platform will thus become, as well as a source of information on NIS good practices, a tool to identify and contact potential right partners for cooperation projects.

OUTCOMES AND DEADLINES

Cooperative projects (Q4 2010)
Country Reports and Who-is-Who Directory (Q3 2010)
Online Platform (ongoing Q2 2010)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Member States: Management Board, National Liaison Officers; PSG; networks of various 'sectoral (private sector) communities' (i.e., in industry, users/consumers and academia, etc.);

RESOURCES FOR 2010 (person months and budget)

- €120,000
- 7 person months

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3c) and d)

2.3 MTP 3: Identifying emerging risks for creating trust and confidence

PROGRAMME NAME :

Identifying emerging risks for creating trust and confidence

DESCRIPTION OF THE PROBLEM TO SOLVE :

Decision makers in both the public and private sector need a clear insight into the nature and impact of emerging and future network and information security challenges in the Information Society. Such challenges are connected to security risks pertinent to emerging and future applications and technologies entering the European market. A better insight in Emerging and Future Risks would allow public and private sector stakeholders to take more appropriate decisions and to have a better basis for policy making.

In 2010, ENISA will deliver risk assessment reports on Emerging and Future Risks for specific application and technology scenarios. The scenarios will reflect the views of various stakeholders across Europe, but will also take account of other ENISA activities in the identification of emerging risks as a transverse issue (e.g. PA1).

DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

In 2008-2009, the Agency has established a framework that will enable stakeholders to better identify and understand Emerging and Future Risks (EFR) arising from new technologies and new applications, which is referred to as the Emerging and Future Risks Framework (EFR Framework). ENISA established expert groups in 2008 and 2009 in order to validate and analyse submitted scenarios from a risk perspective. The ENISA Stakeholder Forum played a prominent role in the ENISA activities on EFR, offering appropriate advice and feedback in steering our activities.

In 2010, the EFR Stakeholder Forum will be continued, and in addition to the Stakeholder Forum, groups of subject matter experts will contribute with their specialized know-how and expertise to the analysis and the identification of EFR (e.g. virtual expert groups, subject matter experts) for selected technologies / applications, as in WP2009. Both groups will be shared with other ENISA activities within WP 2010 (esp. PA1).

By utilizing the EFR Framework, the Agency will support the work programme by preparing risk assessment reports on scenarios taken from areas related to MTP1 and PA1. The ENISA work on EFR is designed to promote a proactive approach in dealing with emerging and future challenges generated by new and emerging technologies and applications. This activity is aiming at boosting trust and confidence in the information society and especially in important areas such as Resilience and Identity and Trust. As such, EFR is developing into a transverse support function for other ENISA MTPs when it comes to identification of emerging risks.

Within this MTP, ENISA will define a process for the identification of topics/candidate scenarios to be analyzed (i.e. a conceptual map for topic selection, scenario selection and communication). This process will help ENISA to identify which scenarios should be analyzed and from which thematic areas.

In support of the activities of the Commission in the area of CIIP, and especially towards pan European exercises, ENISA will make an initial assessment of elements relevant to National Risk Management Preparedness. This will lead to a collection of areas and aspects that are considered to be part of a National Risk Management Preparedness portfolio. Subsequently, identified priority areas/components that can be part of a pan European exercise will be identified (i.e. according to their risk profile). Based on those, various exercise scenarios can be developed. This activity will be performed by a group of European experts in this area (i.e. a working group) and will be coordinated within the framework of the WPK 1.4 activities.

Finally, it is important to note that within this MTP, existing similar initiatives in the area of emerging and future risks/threats but also on CIIP will be taken into account. Interfaces to relevant research programs and activities of the European Commission have been established and ENISA will continue to stay in close contact with EC in order to identify any relevant initiatives (e.g. interaction with Member States with regard to upcoming RFID Recommendation).

WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

Facilitating the Internal Market for e-Communication by assisting European stakeholders to decide the appropriate mix of measures, i.e. technical vs. organisational and legal (noting in particular, the important contribution the Agency can make to the Framework Directive).
Increasing the dialogue between the various stakeholders in the EU on NIS.
Building confidence in the information society through increasing the level of NIS in the EU.

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

SMART goal: By the end of 2010, at least 20 stakeholders or stakeholder organisations from at least 10 Member States refer to ENISA as point of reference for discussing the nature and impact of emerging security challenges in the Information Society.

KPIs: # stakeholders, # Member States

STAKEHOLDERS + BENEFICIARIES

Decision makers in both public and private sector, such as Member States governments, industry, R&D organisations, software developers, system integrators and standardisation bodies who will submit emerging scenarios to be analysed.

WHY ENISA?

ENISA has the capacity to bring the relevant stakeholders together to facilitate discussion and information exchange at European level.

In 2008 and 2009 ENISA made an assessment of information security risks of emerging applications, implemented a roadmap and performed studies on mechanisms to collect, process and disseminate information on emerging risks. At the same time, a number of written position papers on technology trends and risks for emerging areas have been issued and necessary advisory groups have been established (i.e. subject matter experts).

ENISA has established a Stakeholder Forum to play a steering role in the assessment and analysis of Emerging and Future Risks and maintains pool of Subject Matter Experts in for assessing risks of emerging application and technology scenarios.

ENISA is contributing to the area of CIIP and can provide valuable input for pan European exercises.

PROGRAMME PROPOSED BY:

ENISA, Management Board, Permanent Stakeholders' Group

LEGAL BASE

ENISA Regulation, articles 3a), c), d), e), f), g), i) and k)

2.3.1 WPK 3.1- Framework for assessing and discussing emerging and future risks – Analysis of specific scenarios

MTP Name

Identifying emerging risks for creating trust and confidence

WORK PACKAGE NAME :

WPK 3.1: Framework for assessing and discussing emerging and future risks - Analysis of specific scenarios

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

SMART goal: By Q4 2010, above average satisfaction rate (3 on a scale of 1-5, 1=low, 5=max) from stakeholders participating in EFR scenario analysis	**KPI:** satisfaction rate (1-5, 1=low, 5=max)
SMART goal: By Q4 2010, At least two scenarios analyzed	**KPI:** # analyzed scenarios and quality of the assessments
SMART goal: By Q4 2010, at least 6 references to published material on the analyzed scenarios	**KPI:** # references

DESCRIPTION OF TASKS:

The objective of this WPK is to identify emerging and future risks for specific technologies and application areas based on the Emerging and Future Risks (EFR) Framework developed and validated in the previous Work Programme (2008 and 2009). In this context, a number of assessments will be performed to identify Emerging and Future Risks for applications and technology scenarios (referred to as scenarios).

At least two scenarios will be selected according to the indications of our stakeholders (i.e. stakeholders/organisations submitting a request to be analyzed with the ENISA EFR Framework e.g. by the Stakeholder Forum, PSG or virtual group experts). The scenarios to be analyzed will be reviewed in a similar manner as in 2009 and will be prioritised by ENISA committees (e.g. EFR Stakeholder Forum, PSG, ENISA Management Board). In particular, the assessments will identify emerging and future risks in the areas of resilience of information infrastructure and privacy.

To maximise synergies and achieve a bigger impact, the input to be used for the resilience scenario development would be the work carried out within MTP1. Similarly, relevant work by the Commission, and in particular the recent EC RFID recommendation (http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf) will be used as input for the privacy scenario.

In the course of the scenario analysis, policy issues are to be considered, including privacy concerns and other social issues. For this purpose relevant milestones will be defined during the analysis phases to make decisions on the kind of elaboration (i.e. depth, target groups of stakeholders and quality) of policy issues to be addressed. To this extent relevant activities of the European Commission or other policy makers will be taken into account. In addition, this work will be coordinated with relevant work on scenario analysis performed in other work packages (i.e. PA1.1).

Each scenario analysis will be conducted with the support of Subject Matter Experts. For this purpose the reserve lists of subject matter experts established in 2009 will be used; of course new subject matter experts are expected to apply and be included in the reserve lists. A part of the budget will be spent for reimbursement of the involved subject matter experts. The EFR Stakeholder Forum will contribute to this WPK by providing appropriate feedback and supervising the results of the performed work (quality assurance of analysed scenarios, review, comments on the assessment approach).

In this WPK, ENISA will consider and liaise with existing or similar activities taking place at European level, to provide contributions/advice and to avoid any duplication of effort. Interested representatives from DGs of the European Commission can become observer member of the ENISA EFR Stakeholder Forum and will act as liaison between ENISA and DGs on various topics while providing input to our work.

ENISA has already established and will maintain close contact with similar activities and coordination actions funded by the European Commission FP7 framework programme, such as FORWARD and WOMBAT. Information exchange with other EU stakeholders will be also maintained, such as DG ESTAT. Apart from EC activities, other relevant initiatives may be communicated by external experts and/or PSG members whom we envisage to consult throughout the roll-out of our work-programme. For this purpose, a permanent communication channel with experts will be established.

OUTCOMES AND DEADLINES:

At least two risk assessments of selected scenarios (Q3 and Q4 2010) by means of risk assessment reports
Presentation of developed material in security events
Management of Stakeholder Forum and Subject Mater Expert pool

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

ENISA EFR Stakeholder Forum, Industry, academia, standardisation bodies, PSG members

RESOURCES FOR 2010 (person months and budget)

- € 120.000
- 16 person months

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3a), c), d), e), f), g), i) and k)

2.3.2 WPK 3.2 – Maintenance of EFR framework

MTP Name

Identifying emerging risks for creating trust and confidence

WORK PACKAGE NAME :

WPK3.2 – Maintenance of EFR Framework

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

SMART goal: By 2011, at least 2 references in relevant publications and at least one presentation in a relevant event of the predictive model	**KPIs:** # references, #presentations in relevant events, #date
SMART goal: By 2011, at least 2 stakeholders interested in taking up the developed functionality	**KPIs:** # stakeholders participating in the WG

DESCRIPTION OF THE WORK PACKAGE

The objective of this work package is to enhance the functions included in the EFR Framework. Additional capabilities concerning the management and dissemination of collected information, as well as interfaces to other relevant sources (e.g. incidents, threats and vulnerabilities) will be developed. This content of this work package be developed with the advice of an expert group that will be established as an ad hoc Working Group (EFR WG).

The main deliverable of this work package will be a Conceptual map for scenario selection and maintenance of the EFR Framework: Since the EFR Framework is a dynamic process, we expect to use the feedback we collect from its application in WPK3.1 and also from the previous work in WP2009, in order to appropriately update it, with a view to improving its functionality. Of particular importance will be the update of the process regarding the identification and selection of appropriate areas and scenarios (technologies and applications) that initiates the whole process; the idea behind this being that there should be a conceptual model in place underlying this selection, which would assist in properly identifying and selecting a scenario together with the relevant area (i.e. technology driven vs. other approaches such as policy, societal issues etc.). This is essential since the identification of a proper scenario is critical for the achieved impact and as such is an important success factor for this work.

This result will contribute towards the fast transparent and systematic identification of thematic areas and scenarios.

OUTCOMES AND DEADLINES:

- A conceptual model and a process for thematic area and scenario selection (by Q1 of 2010) including weighting and prioritisation scheme.

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

MB, PSG, NLOs, Working Group members (industry, academia, research), EFR Stakeholder Forum

RESOURCES FOR 2010 (person months and budget)

- 35.000 €
- 3 person months

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3a), c), d), e), f), g), i) and k)

2.3.3 WPK 3.3 – Enhancing national risk management preparedness

MTP Name

Identifying emerging risks for creating trust and confidence

WORK PACKAGE NAME :

WPK3.3 – Enhancing National Risk Management Preparedness: in support of pan European exercise

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

SMART goal: identification of European experts in the area of National Risk Management Preparedness.	**KPIs:** # of experts involved in the working group.
SMART goal: By the end of 2010, a list of main areas that should be considered as part of National Risk Management Preparedness towards CIIP will be identified. Based on this material, a list of relevant CIIP related areas/components will be identified and documented (based on risk aspects). This will serve as basis for exercise scenarios.	**KPIs:** completeness of the list with topics relevant to National Risk Management preparedness will be developed. Based on identified areas/components, exercise scenarios will be developed.
SMART goal: By the end of 2010, at least two Member States will be interested in the results and willing to follow up on this.	**KPIs:** # of interested Member States.

DESCRIPTION OF THE WORK PACKAGE

CIIP and resilience of communication networks is an area that involves many stakeholders and many areas, from technology to policy and inter-organisation coordination and communication. Proactive management of information risks is a key issue in building up and maintaining resilient information infrastructures. When looking at the elements of risks pertaining information assets (both technical and organisational), different aspects have to be taken into account, depending on the nature, importance and impact this information has in a CIIP context. Furthermore, when considered at the level of a Member State, the establishment/enhancement of National Risk Management preparedness has to involve multiple stakeholders from both private and public sectors.

With this work package we aim at the initial identification of areas that can be considered as necessary for National Risk Management Preparedness, as well as the identification of involved stakeholders from EU Member States. Issues related to CIIP will be the main element for the identification of these areas, whereas other, directly related areas will be considered as well. Important dependencies between these areas and main components will be in focus. The final result will be a first picture of areas and components, involved stakeholders and their roles for National Risk Management Preparedness.

This will be achieved by building up a Working Group of national experts in the area of Risk Management, covering public and private organisations. The task of this Working Group will be the identification and description of all relevant elements of National Risk Preparedness for public eCommunication network resilience. This will include various relevant elements, for example, related components (e.g. types of infrastructures under protection), related stakeholders (e.g. owners/operators of infrastructure, regulators, public/private emergency groups etc.), users of the infrastructure, related critical areas this infrastructure is used for (e.g. energy, health, etc.), risk management responsibilities of each involved stakeholder, necessary coordination activities, necessary national escalation schemes, etc. A first ranking of these elements according to their value, impact and risk profile will be made.

The produced material will flow into the work of WPK 1.4 and will support the definition of scenarios as they are required towards pan European resilience exercises. To this extent, interfacing this activity with activities of MTP1 will be necessary, both concerning the coordination of the Working Group but also timing and structure of the deliverables of the WG.

Having this information, interested stakeholders will be in the position to track national developments in this area and decide upon necessary activities for the establishment/enhancement of National Risk Management Preparedness. In addition, this information will build the basis for stock taking activities in different Member States and the identification of road map for future actions in that area. Concerning pan European resilience exercise, the delivered list of various CIIP related elements based on recognised risks will be an important contribution towards the definition of exercise scenarios.

OUTCOMES AND DEADLINES:

- Documentation of the identified elements/areas of National Risk Management Preparedness. (by Q4 of 2010)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

MB, PSG, NLOs, European Commission, Member States, Subject Matter Experts (industry, academia, research)

RESOURCES FOR 2010 (person months and budget)

- 80.000 EURO
- 11 person months

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3a), c), d), e), f), g), i) and k)

2.4 PA1: Identity, accountability and trust in the future Internet

THEME NAME :

PA1: Trust and Privacy in the Future Internet

DESCRIPTION OF THE PROBLEM TO SOLVE :

With the advent of the Internet each person has the opportunity of living two lives in parallel in the real as well as in the virtual world. A trend observed over the last few years, first in the research community, but now also in commercial offerings is the increase of interactions between these two worlds, making real-world information accessible to services on the Internet. This will lead to a situation where sensor and actuator nodes will account for the majority of connected nodes in the Future Internet forming its "Real World" part, while at the same time increasing the amount of information searchable and accessible via the Internet. In addition to the Real World Internet, the Internet of Things (IoT) forms another parallel development line in the Future Internet. As an evolution of today's RFID technology, the IoT consists of networks of nodes that interact with objects bearing tags.

The Future Internet (FI), whilst still layered, will be affected by a number of cross-cutting dependencies, leading to an increased complexity and distributed responsibility. It will exhibit a multitude in scale compared to the current Internet, mainly due to the vast extension of scope, caused by the inclusion of a multitude of connected entities of different types. The FI is likely to develop spontaneous and emerging behaviours and unanticipated new usages. The appearance of new entities, services and business scenarios will rather be the rule than the exception. It will evolve into a pervasive, digital environment, composed of multiple interconnected heterogeneous infrastructures, terminals and technologies. Users will interact by means of the FI throughout their lifetime, in varying roles and in different communities and socio-economic contexts. Each of these situations will impose the usage of different identities, protection needs and trust requirements.[9]

Without any doubt security, privacy, and trust are crucial for any service, application and transaction offered over public communications network. Their importance is expected to increase even more in large distributed systems providing links to the real-world, as the Future Internet is expected to do. In this context, ensuring integrity of information, protecting the source of information and establishing trust (with persons as well as objects, sensors and actuators) are some of the key challenges that have to be addressed.

DESCRIPTION OF THE APPROACH TAKEN SOLVING THE PROBLEM:

The overall goal of this Preparatory Action is to "ensure that Europe maintains a high level of security and confidence of both users and industry on the ICT infrastructure and provided services, while at the same time limiting the threats to civil liberties and privacy".

ENISA will reach this goal through:
1) Reviewing and assessing the potential impact and consequences of threats arising from the introduction of emerging technologies and identifying the role of trust and accountability (including trust in infrastructures). ENISA will study models of electronic services related to security and, in this respect, consider available methods for the user-consented management of personal data and their revocation, the propagation of user-consented management methods in multiple environments and their possible use in Future Internet services scenarios.

[9] Position Paper on Trust & Identity in the Future Internet, Future Internet Assembly, Madrid, 9th December 2008

2) Follow the development and deployment of technologies that enable privacy-preserving access to data, mechanisms to ascertain minimal disclosure, advanced identity schemes, privacy-friendly identity service provision, policy requirements and enforcement, and usage control based on trusted computing and end-to-end security. Perform a stock-taking exercise looking at important trends and/or privacy issues.

3) The development of policy and good practice initiatives aiming towards achieving a balance among Transparency, Accountability and Responsibility. This also includes the development of requirements on the approximation of existing models of electronic authentication as well as the development of guidelines and recommendations for necessary regulations, with regard to privacy and trust, as it might be appropriate, and a governance model concerning supervision and accreditation.

4) Cooperate closely with the Commission (and with DG INFSO.F5 and DG INFSO.H2 in particular, so as to ensure regular exchange of information and exploitation of any synergies that are identified as the initiative progresses.

ENISA will carry the preparatory work for the next years by reviewing a number of technologies in the area, their deployment status and respective policy initiatives relevant to trust and privacy.
Given the complexity of the subject, this Preparatory Action will expand on two years, 2010 and 2011.

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

SMART goal: By 2012, the Commission and at least 50% of the Member States have made use of ENISA recommendations in their policy making process

KPIs: Commission (yes/no), % of Member States

WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

Building confidence in the Future Internet of both the public and ICT industry in the EU
Facilitating the Internal Market for e-Communication by assisting the institutions to decide the appropriate choice of regulation and measures to undertake.
Increasing the dialogue between the various stakeholders in the EU on privacy and trust (including trust and confidence on infrastructures).
Increasing co-operation between MS in order to reduce the differences of policy initiatives between them.

STAKEHOLDERS + BENEFICIARIES

National Regulatory Authorities, Member States Governments and EU Policy and Decision Makers, network operators and service providers, associations of providers and auditors, network equipment vendors

WHY ENISA?

ENISA is well positioned in ensuring a high level of security and confidence of both the public and industry on the ICT infrastructure and provided services.

By its nature the Internet extends beyond national border, hence the challenges cannot be addressed neither "in isolation" nor without co-ordination between EU MS. By its designation, ENISA is well-positioned to promote and facilitate European Union joint policies, activities, and procedures in this area.

2.4.1 WPK PA1.1 – Stock taking of authentication and privacy mechanisms

MTP Name

Trust and Privacy in the Future Internet

WORK PACKAGE NAME :

WPK PA1.1: Stock taking of authentication and privacy mechanisms

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

SMART goal: References to the deliverables > 5	**KPI:** # Number of references
SMART goal: Member states participating in stock taking exercises > 20	**KPI:** # Number of Member States

DESCRIPTION OF THE WORK PACKAGE

The notion of identity in ICT applications and services is evolving rapidly, while many related concepts like “trust” could have a profound effect on the way in which infrastructure and services will be secured in the future. The success of social networking sites among other things demonstrates that there is considerable scope for abuse through the inappropriate use of personal information. Not addressing these concerns will result in the loss of confidence by the public in the ICT services and would hinder innovation and growth.

The previous work performed by ENISA in this area indicated that one of the biggest obstacles to overcome in the medium term is the difference of security and privacy requirements within the EU member states for different applications. ENISA will continue its work on this topic by collaborating with leading European initiatives, amongst others IDABC, the STORK consortium and CEN working groups. In this respect the aim will be to identify the foundations required to establish secure services across Europe, which will result in best practices and recommendations for technologies related to secure services and electronic authentication, authorisation and accounting. In this context, several authentication methods including web-based ID frameworks and authentication methods based on hardware tokens need to be compared taking into account the requirements of important electronic services in Europe.

Another area of particular interest is the management of multiple identities. In this context, “identity” is being considered in a broad sense (i.e. eID, Federated identity, RFID, avatars, etc.). Possible application environments for investigation are virtual on-line worlds where the notion of anonymity could be explored.

Finally, the introduction of a European data breach notification requirement for the electronic communication sector introduced in the review of the ePrivacy Directive (2002/58/EC) is an important development with a potential to increase the level of data security in Europe and foster reassurance amongst citizens on how their personal data is being secured and protected by electronic communication sector operators. Against this background, ENISA aims to review the current situation and to develop a consistent set of guidelines addressing the technical implementation measures and the procedures as described by Article 4 of the reviewed Directive 2002/58/EC.

OUTCOMES AND DEADLINES:

- Report identifying methods for the management of multiple identities (Q4 2010).
- Report presenting the state-of-the-art in the deployment of eIDs in private and public sectors in the Member States, identifying trends and possible incentives (Q4 2010)
- Stock taking of existing practices on current data breach notification among in various sectors (Q4 2010)

The next steps related to above mentioned activities, to be performed in 2011 in case this Preparatory Action is transformed into a Multiannual Thematic Programme, include:

- Best practices and recommendations for technologies related to secure services and electronic authentication
- Guidelines on the technical implementation measures and procedures as described by Article 4 of Directive 2002/58/EC

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Networking equipment vendors, National Regulatory Agencies (NRAs), Service providers, Industrial R&D institutions, Universities and Research centres, European Technology Platforms.

RESOURCES FOR 2010 (person months and budget)

- 9 person months[10]

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3a), b), c), f), and k)

2.4.2 WPK PA1.2 – Stock taking of service models supporting electronic services

MTP Name

Trust and Privacy in the Future Internet

WORK PACKAGE NAME :

WPK PA1.2: Stock taking of security models supporting electronic services

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

SMART goal: Identification and assessment of service models >5	**KPI:** # Number of assessed service models
SMART goal: References to the deliverables > 5	**KPI:** # Number of references

[10] At the moment of preparing this document the Agency can not commit financial resources in this Preparatory Action. Nevertheless, the required resources (€90,000) could be obtained in the course of the year.

DESCRIPTION OF THE WORK PACKAGE

The main objective of this activity is to perform a stock taking exercise on existing models of electronic services and their security characteristics, assessing the balance between privacy and accountability, consent and tracking that they present. Today's online application environments are characterised by a plethora of "customized" security models tailored to the various classes of applications in which they operate. There is a need to examine how users should use different types of electronic services.

In 2010 ENISA will study security models of electronic services and their performance in highly distributed environments, such as today's Internet. Furthermore, ENISA will investigate various ways of assuring privacy and accountability in the Internet, review the most prominent methods used, study their mapping to the underlying architectures and assess their level of effectiveness and performance. ENISA will also work towards the development of recommendations on the use of specific service models in given environments and architectures. This will also entail the development of guidelines for necessary actions with regard to privacy and trust.

OUTCOMES AND DEADLINES:

- Catalogue of current service models and their security issues in different architectures (Q4 2010).
- Evaluation of identified service models and recommendations for specific architectures (Q4 2010)

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

National Regulatory Agencies (NRAs), European Commission, Service Providers, Universities and Research centres, EDPS, European Technology Platforms.

RESOURCES FOR 2010 (person months and budget)

- 9 person months[11]

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3a), b), c), f), and k)

[11] At the moment of preparing this document the Agency can not commit financial resources in this Preparatory Action. Nevertheless, the required resources (€90,000 for workshops, consultancies, running of the experts groups, electronic and printed publications) could be obtained in the course of the year (i.e. contribution from EEA Countries).

2.5 PA2: Identifying drivers and frameworks for EU sectoral NIS Cooperation

THEME NAME :

PA2: Identifying drivers, barriers and frameworks for EU sectoral NIS cooperation

DESCRIPTION OF THE PROBLEM TO SOLVE:

A growing number of network and information security (NIS) threats involve sophisticated combinations of network and service protocols. Traditional forms of protection based simply on strong "firewalls" around individual corporate networks are no longer enough to prevent intruders from entering and stealing or damaging key electronic assets of businesses or other organisations. This creates a fundamental challenge to organisations doing business online, and cooperation between network and service providers in NIS service development and provision has grown as a result of market demand for solutions to the problem.

As intangible assets have become increasingly core to value generation, technologically advanced companies, both large and small, have also found good reasons for working on NIS challenges with public agencies. Individual companies of course have some legal obligations to cooperate with public authorities in such areas as data protection and retention. But the complex and sometimes legally ambiguous nature of NIS attacks (at least initially) mean that more voluntary, comprehensive and proactive forms of cooperation amongst sectors along supply chains may need to be increased if exploitation of possible gaps in supply chain security are not to cause potentially widespread economic disruption.

To be successful, however, such forms of cooperation need to be based on a realistic assessment of the respective parties' ability to tackle NIS challenges in relation to their legitimate commercial or regulatory responsibilities and capabilities. Otherwise, responses are liable to be fragmented, inadequate or disproportionate and potentially unrealistic in terms of what those involved either need or can deliver.

Yet problems for a broad range of important public policy issues could be generated by solely supply-side cooperation if demand-side drivers are not positively delineated, or market failures clearly identified. However, very little is known about the operational, commercial and/or regulatory conditions that actually deter, facilitate or incentivise NIS cooperation between different sectors, and the kinds of situations where cooperation with public sector authorities in the development of service tools, services or cooperative frameworks may be mutually useful or desirable from a commercial and public policy perspective.

If organisations are to face coherent, straightforward and effective regulatory requirements and public-private coordination optimised, national, EU and international approaches need to be integrated. The increasing complexity of security threats means they are rarely capable of being dealt with by any single entity at any one level. Action by actors with different areas of responsibility at any one level may impact on the ability of others to take action, potentially undermining overall effectiveness. Attempts to cooperate at pan-European and international levels may also face potential contradictions with national regulatory requirements unless partnerships are given explicit legal sanction or support by public sector agencies at EU and international levels.

Though general incentives for cooperation amongst private sector and between public-private sectors may be quite extensive, barriers to their successful development may also be quite strong. Analysis of these barriers can help identify how pan-European frameworks could create commercial, economic and regulatory incentives for various supply chain actors (network operators, software and service providers, user organisations and public agencies) to cooperate with each other in ways that facilitate market drivers where they exist, and are in line with the full range of public policy requirements where there are market failures. The PA proposed here will thus seek to clarify the question of how best to get commitments from relevant actors to collective action to address NIS challenges at a pan-European level.

DESCRIPTION OF THE APPROACH TAKEN TO SOLVING THE PROBLEM:

The PA will identify where commercial, economic and/or regulatory barriers and drivers to sectoral cooperation, and incentives for public-private sector partnerships, are stronger or weaker in the development of a number of supply chain NIS services. As described in WPK PA2.1, work will start by identifying the NIS service requirements of private sector actors in two or three different sectors. These requirements will be considered in relation to ENISA's existing work on CII Resilience, and PA's commercial and economic orientation will complement the more operational and technological orientation of the work in WP2010 MTP1 through focusing on the demand-side requirements for cooperation of businesses as intermediate or end-users of end-to-end supply chain NIS services. The relation between the general and sector-specific issues will be developed through the following steps:

1. Identification of the general threat, business model and market conditions that can lead demand-side actors in different sectors (both large and SME business network-based service users) to require increased inter-sectoral cooperation in key NIS issues;
2. Identification of the ways and extent to which these requirements can lead to the need for specific responsibilities, commitments and rewards for infrastructure, software and service security providers;
3. Identification of the particular good practice tools, services or cooperative frameworks that could be developed between public and private sector actors at a pan-European level to meet these requirements.

These steps will be iterated in relation to, amongst other initiatives, ENISA's existing engagement in Brokering an Financial Information Sharing and Alert and Community (FI-ISAC), in developing an online tool for Micro-enterprises and the Swedish/Dutch Multipurpose Information Managements and Exchange for Robustness (MIMER) project. This will be facilitated through engaging ENISA's PSG members – both as individuals and in drawing in other representatives from their constituencies - as well as from ENISA's Stakeholder Relations section's other sector and national trade association networks.

The bulk of the work for the PA will be done as outlined in WPK PA2.1. In addition, over Q1 and Q2 2010, the Agency will conduct an analysis of key issues in national, EU and international NIS cooperation structures for public and private sector actors. This analysis coordinated closely with the network resilience work and analysis in MTP1, along with an independent report based on in-depth interviews with key Member State and private sector representatives involved in cooperative ventures by a consultant and the Country Reports and Who-is-Who Directory in WPK2.3. The objective of this exercise would be to clearly assess where ENISA engagement could best support Commission and MS policy objectives going forward.

The report and assessment (including of WPK PA2.1) would be developed and tested through 3 workshops involving supply chain participants from the 2-3 different sectors and held during Q2 and Q3 2010 and hosted by Member States or held at ENISA. In Q4 2010, ENISA would then bring together the relevant stakeholders for a final workshop to assess the overall conclusions of the work and to suggest possible further action lines beyond 2010.

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

SMART goal: Identification of where commercial, economic and/or regulatory barriers and drivers to sectoral cooperation, and incentives for public-private sector partnerships, are stronger or weaker in the development of a number of supply chain NIS services.

KPI: Participation in the development of cross-sectoral cooperative initiatives in at least 3 supply chains across at least 2 EU MS.
KPI: Identification of requirements for public sector involvement in development of good practice tools, services or cooperative frameworks by demand-side actors in at least 2 supply chains.

SMART goal: Identification of how cooperative initiatives could be developed in at least 2 areas of ENISA work post 2010.

KPI: number of good practice tools, services or cooperative frameworks identified to be followed up in ENISA work beyond 2010.

WHICH HIGH-LEVEL GOALS THE PROGRAMME SUPPORTS:

- Facilitating the Internal Market for e-Communication by assisting the institutions to decide the appropriate choice of regulation and measures to undertake.
- Increasing the dialogue between the various stakeholders in the EU on network resilience, service and software security, privacy and trust.
- Increasing co-operation between MS in order to reduce the differences of policy initiatives between them.
- Building confidence in the Future Internet of both the public and private sectors in the EU.

STAKEHOLDERS + BENEFICIARIES

Member State and EU Policy and Decision Makers; National Regulatory Authorities; PSG; businesses in pan-EU supply chains; various ‘private sector communities’ in industry, users/consumers and professional organisations.

WHY ENISA?

ENISA is well positioned to achieve a high level of confidence of both public and private sector actors in the development of a cross-sectoral approach to the development of a framework for pan-EU NIS cooperation because of the multi-stakeholder representation in the PSG, its existing networks of business and professional groupings (at EU and national level) and its existing work in ICT infrastructure and services security. It is the only official agency capable of addressing issues to do with pan-EU supply chains, and the gaps in cooperation models that may exist at this level, and has existing engagement in or with the international bodies addressing the relevant issues (OECD, ICANN, ITU and 3rd Countries).

RESOURCES FOR 2010 (person months and budget)

- €105,000
- 10 person months

2.5.1 WPK PA2.1 – Incentives and responsibility requirements for multi-stakeholder NIS governance frameworks in ICT supplier and user communities

MTP Name

Drivers and Frameworks for EU Sectoral NIS Cooperation

WORK PACKAGE NAME :

WPK PA2.1: Incentives and responsibility requirements for multi-stakeholder NIS cooperation in ICT supplier and user communities

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

SMART goal: Identification of the threat conditions that incentivise private actors to develop cooperative frameworks for shared NIS responsibilities with public sector actors at a pan-European level.	**KPI:** Participation in the development of a pan-EU framework with the public sector by private actors in at least two sectors from at least 2 EU MS.
SMART goal: Identification of the commercial and market conditions that, for demand-side firms (large companies and SMEs), may lead to a need for a public-private framework for cross-sectoral NIS cooperation.	**KPI:** Market failure in cross-sectoral provision of NIS services for at least two demand-side sectors in large corporate and/or SME markets in at least 2 EU MS.
SMART goal: Identification of relevant good practice tools or services that need to be developed to support the functioning of such cooperative frameworks.	**KPI:** Number of good practice tools and/or services identified to support cooperative frameworks for large or small companies in at least 2 sectors.

DESCRIPTION OF TASKS:

A first task of this PA is to identify where barriers and incentives to cross-sectoral NIS cooperation are stronger or weaker, the possibility of success in the short or medium term greater or more challenging, and the need for public-private sector partnerships thus potentially more or less necessary. This Work Package will therefore investigate the NIS requirements of different groups of private sector actors, and the incentives for engagement in multi-stakeholder frameworks by them.

In particular, it will investigate how the NIS requirements of business users of network-based services may or may not affect cooperation between software and service providers and network operators in the development and delivery of NIS services. In at least one supply chain it will aim to distinguish between the success of service provision and supply-side cooperation for large business users in relation to SMEs. For the latter, it will also be explored whether the participation of multiplier organisations in defining the requirement of SMEs (rather than them simply engaging with NIS service providers individually) can augment the ability to leverage change.

Finally, it will identify whether, in cases where the requirements of users are not being met, the involvement of public sector actors in developing good practice tools or services may facilitate the cross-sectoral cooperation required by users.

Over Q1 and Q2 2010, the Agency will conduct two studies of the NIS requirements of business users, including high-tech SMEs in at least one of these. Both these studies will be of these sectors in at least two Member States.

The draft studies, including preliminary findings, will feed into the 2 workshops organised under the general PA2 rubric, to be held during Q2 and Q3 2010 and hosted by Member States or held at ENISA. In Q4 2010, ENISA would then bring together relevant stakeholders for a final workshop to assess the overall conclusions of the work and to suggest possible further action lines beyond 2010.

OUTCOMES AND DEADLINES

- Sectoral demand-side studies Q1, Q2
- Consultant's report Q4
- Workshops Q2, Q3, Q4

STAKEHOLDERS NEEDED TO ACTIVELY SUPPORT THE WORK PACKAGE

Member States: Management Board, National Liaison Officers; PSG; Networks of various 'topical (private sector) communities' (i.e., in industry, users/consumers and academia , etc.), individual companies

RESOURCES FOR 2010 (person months and budget)

- €105,000
- 10 person months

WORK PACKAGE PROPOSED BY:

ENISA

LEGAL BASE

ENISA Regulation, articles 3c) and d)

Summary of Multi-annual Thematic Programmes and Work Packages

MTP 1	**Improving resilience in European e-Communication networks**	**Budget line**	**Budget**	**Person months**	**New Activity**
WPK 1.1	Underpin stakeholders' efforts to deploy ENISA's information sharing and incident reporting good practice guides.	3510	100.000	11,5	Revised
WPK 1.2	Assist providers in enhancing the resilience of their networks.	3510	150.000	13,5	Revised
WPK1.3	Investigation of innovative actions	3520	195.000	17,5	NO
WPK 1.4	Empower stakeholders towards the first pan European exercise.	3520	100.000	13,5	Revised
	TOTAL		**545.000**	**56**	
MTP 2	**Developing and maintaining co-operation models**	**Budget line**	**Budget**	**Person months**	**New Activity**
WPK 2.1	Co-operation platform for awareness raising community	3310	60.000	24	NO
WPK 2.2	Security competence circle and good practice sharing for CERT communities	3300	135.000	24	NO
WPK 2.3	European NIS good practice Brokerage	3320	120.000	7	NO
	TOTAL		**315.000**	**55**	
MTP 3	**Identifying emerging risks to create trust and confidence**	**Budget line**	**Budget**	**Person months**	**New Activity**
WPK 3.1	Framework for assessing and discussing emerging and future risks – Analysis of specific scenarios	3500	120.000	16	NO
WPK 3.2	Maintenance of EFR Framework	3500	35.000	3	NO
WPK 3.3	Enhancing national risk management preparedness	3500	80.000	11	YES
	TOTAL		**235.000**	**30**	
PA1	**Identity, accountability and trust in the future Internet**	**Budget line**	**Budget**	**Person months**	**New Activity**
WPK PA1.1	Monitoring and assessing of risks and threats on resilience, privacy and trust arising from the introduction of emerging technologies	3520	0	9	YES
WPK PA1.2	Development of policy initiatives aiming towards achieving a balance between privacy, accountability, consent and tracking	3520	0	9	YES
	TOTAL		**0**	**18**	
PA2	**Identifying drivers and frameworks for EU sectoral NIS cooperation**	**Budget line**	**Budget**	**Person months**	**New Activity**
WPK PA2.1	Incentive and responsibility requirements for multi-stakeholder NIS governance frameworks in ICT supplier and user communities	3520	105.000	10	YES
	TOTAL		**105.000**	**10**	
	TOTAL (All MTP)		**1 200.000**	**169**	

3 HORIZONTAL ACTIVITIES

The Agency will perform a number of activities required for its functioning in addition to the thematic Multi-annual Thematic Programmes. This includes developing ENISA strategy and public affairs management, managing ENISA bodies and groups, managing relations with external stakeholders, measuring the uptake of ENISA deliverables, managing the Agency's internal capabilities, internal communication and Work Programme development.

3.1 Developing ENISA strategy and public affairs management

The Agency will develop a strategy for the period until 2012 and beyond. Strategic requirements for the development of the annual Work Programmes will be established in parallel with the WP development process.

The Agency will conduct communication and outreach activities to support the impact of it's work. In 2010, the Agency will manage its corporate communication channels and reach out to NIS experts. Corporate communication activities have been restructured under the following budget lines: Communications Activities (EUR44.000), ENISA corporate website (EUR20.000), General Report on ENISA activities and other publications (EUR40.000). Outreach to NIS experts will be achieved through the ENISA Quarterly (EUR40.000), co-organised events (EUR30.000) and speaking engagements of ENISA experts at conferences and events (which does not require any additional budget).

Legal base: ENISA Regulation, articles 2.3 and 3a), e), f) and k) and 7.5a)

3.2 Managing ENISA bodies and groups

The Agency will organise meetings of the Management Board (EUR110.000) and the Permanent Stakeholders' Group (EUR100.000, including informal MB/PSG meeting). Co-ordination of Working Groups' activities and management of the network of National Liaison Officers have been included in MTP activities..

Legal base: ENISA Regulation, articles 5, 6, 7.4g), h), and i), and 7.8

3.3 Managing relations with external stakeholders

The Agency, in close cooperation with Commission services, will maintain and continue to develop relationships with 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. ENISA will also identify common areas of interest and assess to which extent collaboration with such actors in specific activities of the Agency is feasible (e.g., facilitating dialogue on secure software development between industry and Commission as legislator). These activities require EUR410.000 for staff missions, EUR5.000 for representation costs, EUR3.000 for meetings of the Executive Director and EUR10.000 for other meetings.

Legal base: ENISA Regulation, articles 3c) and j) and 7.4g and h)

3.4 Managing internal capabilities

"The Agency will continue to maintain and expand its Who-is-Who database with public and private sector contacts (EUR0). The Agency will continue its activities on internal risk management and information security by developing an internal audit capability (EUR25.000). In addition, the Agency will maintain its ability to make translations (EUR20.000) of official financial documents."

Legal base: ENISA Regulation, article 7.4d)

3.5 Managing ENISA internal communication

The Agency highly values information sharing and co-operation between its staff and management and among all staff in general. For this purpose, the Agency has established various internal communication channels and as such will frequently issue its ENISA Inside flyer, organise weekly internal staff meetings and information sharing through its own intranet.

Legal base: ENISA Regulation, article 7.4d) and f)

3.6 Work Programme development

Each year, the Agency draws up its annual Work Programme. The programme is subject to consultation with the Permanent Stakeholders' Group and decision by the Management Board. In principle, this activity does not require any budget.

Legal base: ENISA Regulation, article 7.5b), 7.6 and 9

Summary of Horizontal Activities

HA 1	Providing advice and assistance	Budget line	Budget	Person months	New Activity
HA 1.1	Co-ordination of request handling	3320	0	0.5	NO
HA 1.2	Response to request	3320	0	0.5	NO
	TOTAL		**0**	**1.0**	

HA 2	Communicating and reaching out to NIS stakeholders	Budget line	Budget	Person months	New Activity
HA 2.1	Strategy Development	p.m.	0	2.0	Revised
HA 2.2	Public Affairs Management	p.m.	0	10.5	Revised
HA 2.3	Communications Activities	3210	44.000	5.5	Revised
HA 2.4	ENISA corporate website	3220	20.000	21	NO
HA 2.5	ENISA General Report & Publications	3210	40.000	6	NO
HA 2.6	ENISA Quarterly	3211	40.000	4	NO
HA 2.7	Co-organised events	3200	30.000	4	NO
HA 2.8	Speaking engagements	n.a.	0	11	NO
	TOTAL		**174.000**	**64**	

HA 3	Managing ENISA bodies and groups	Budget line	Budget	Person months	New Activity
HA 3.1	Management Board	3003	110.000	4	NO
HA 3.2	Permanent Stakeholders' Group	3000	100.000	4	NO
HA 3.3	Co-ordination of Working Groups	N/A	0	2	NO
HA 3.4	National Liaison Officers Network	N/A	0	2	NO
	TOTAL		**210.000**	**12**	

HA 4	Managing relations with external stakeholders	Budget line	Budget	Person months	New Activity
HA 4.1	Developing relations with industry, academia, consumer representatives and International Institutions and Third Countries	3330	0	4.5	NO
HA 4.2	Managing relations with EU Bodies	3320	0	3.5	NO
HA 4.3	Missions Executive Director	3015	35.000	0	NO
HA 4.5	Missions Operational Departments	3013	345.000	0	NO
HA 4.6	Missions Administration Department	3014	30.000	0	NO
HA 4.7	Representation costs	3011	5.000	0	NO
HA 4.8	Meetings of Executive Director	3005	3.000	0	NO
HA 4.9	Other meetings	3021	10.000	0	NO
	TOTAL		**428.000**	**8**	

Continued over page

Summary of Horizontal Activities (continued)

HA 5	Managing ENISA internal capabilities	Budget line	Budget	Person months	New Activity
HA 5.1	Who-is-Who database	3320	0	0	NO
HA 5.2	ENISA Internal Audit Capability	3400	25.000	1	NO
HA 5.3	Translations	3230	20.000	0	NO
	TOTAL		**45.000**	**1**	
HA 6	**Managing ENISA internal communication**	**Budget line**	**Budget**	**Person months**	**New Activity**
HA 6.1	ENISA internal newsletter, staff meetings, information sharing through intranet	N/A	0	4	NO
	TOTAL		**0**	**4**	
HA 7	**Work Programme development**	**Budget line**	**Budget**	**Person months**	**New Activity**
HA 7.1	Development of 2011 Work Programme	N/A	0	10	NO
	TOTAL		**0**	**10**	
	TOTAL (Horizontal Activities)		**857.000**	**100**	

4 PROVIDING ADVICE AND ASSISTANCE

Since 2006, the Agency has received requests coming from the Member states (8), from the EC (6) and other European bodies (2) (see table below). Such requests are also expected to emerge in 2010. This confirms the role foreseen for ENISA in articles 2, 3 and 10 of the Regulation.

Article 6 of the Internal Rules of operation for the handling of requests specifies the procedure for handling incoming request. For eligible requests, the Agency will set priorities on the basis of criteria, such as availability of resources, continuity of long-term actions, existing commitments and expected added value and impact at EU level of the response to the request.

In principle, incoming requests will be handled on a first-come-first-serve basis. In case of need, the Executive Director will consult without delay the Management Board before taking a decision on priorities.

Requests handled between December 2005 and June 2009

Requestor	Subject	Budget [Euro]	ENISA staff [Person months]
1) EDPS	Facilitating audit of EURODAC System	3,400	1.6
2) Commission	Assessment of security measures taken by electronic communication providers	0	2.2
3) NRA Lithuania	Assistance in setting-up of CERTs through organising a CERT training in Lithuania	6,745	0.8
4) Commission	Providing feedback on Impact Assessment on planned Communication	0	1.3
5) Commission	Advice on mid-term review of Directive on Electronic Signatures	850	0.5
6) Commission	Advice on eID management in Commission services	850	1.1
7) Czech Republic	Assessment of security requirements for Public Administration Information Systems	0	0.6
8a) Commission	Examining the feasibility of a data collection framework	50,000	6.0
8b) Commission	Examining the feasibility of an EU-wide information sharing and alert system	25,000	4.0
9) Greece	Advice on telephony encryption	0	0.1
10) Austria	SBA-ENISA co-operation	0	0.1
11) Austria	Risk management and analysis questionnaire	0	0.1
12) Bulgaria	Facilitating Hungarian-Bulgarian cooperation to set up Bulgarian Government CERT	0	0.1
13) Greece	Creation of CSIRT at FORTH-ICS	0	0.1
14) Austria	Assistance in setting-up of CERTs through organising a CERT training	6,745	0.8
15) Eur. Parliament	Advice on Internet security matters	0	0.5
16) Cyprus	Assistance in setting-up a governmental CERT	0	0.5

5 ADMINISTRATION ACTIVITIES

The Administration Department seeks to ensure compliance and further reassure the functionality of the administrative procedures of the Agency in order to deliver dependable services. In 2010 the goals of the Administration Department is to enhance the range and quality of services available in line with the compliance objectives that have been instantiated in the internal control standards and audit results. In this regard electronic workflows will be made available further in new areas of activity; further mitigation of risks will take place in order to ensure business continuity. In 2010, the Administration Department seeks to:

- Enhance the range and quality of services available
- Mitigate compliance risks
- Ensure business continuity

In 2010 the Administration Department seeks to further interact with horizontal services sections and functions such as Accounting and Internal Control. The Work Program 2010 continues referring to the activities of these two functions next to the planning of the activities of the Administration Department.

5.1 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 2010 the priorities of General Administration include:

- Multi-annual planning of activities
- Monitoring of annual budget execution
- Planning of electronic workflows
- Mitigation of compliance risks
- Ensuring business continuity

The main activities planned for 2010 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 HoTCD 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

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
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.	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, office management, safety & security, post, vehicle.	Volume of activities Timely execution	On going	384,000
1.7	Relations with Hellenic Republic Authorities	Regular contacts and advice to the ED on relations with host Member State	Number of cases handled Timely responses	Ongoing	0
1.8	Handling requests of Staff members related to the implementation of the seat agreement (special ID cards, car registration, VAT exemption etc).[12]	Regular handling of VAT exemption requests for the Agency's Staff	Number of cases handled Timely responses	Ongoing	0

[12] See, activities of the Directorate regarding Relations with Hellenic Republic authorities.

5.2 Finance

The Finance Section 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 2010 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).

The main activities planned for 2010 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
2.1	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 December. Preparation by 10 December.	0
2.2	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
2.3	Annual budget reports	Monthly	Budget status reporting for al areas, Titles and Department, as necessary, including analysis of main relevant aspects.	Monthly (for the previous month)	0
2.4	Organising carryovers	Support the Departments in dealing with carryovers	Communication Time and control	Annually by end of second week of the year	0
2.5	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

5.3 Human Resources

HR activities at ENISA include recurrent tasks, and general activities particularly related to recruitments, performance evaluations, training, health and safety at work, leave management handling of individual rights and payroll management. The goal of HR is to ensure timely recruitment and staff retention policies in line with the Staff Regulations.

In 2010 the scope of HR is to consolidate the organisational changes of 2009 that mark a shift towards greater hierarchical control of the Agency when executing upon operational goals at the MTP level. In 2010 the priorities of the HR Section include:

- Recurrent resource planning (Staff Policy Plan)
- 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 EC Management Costs	Monthly Payroll and employer duties carried out on time. Individual rights. Grading Committee. EC Management Costs	Administer Title 1 and payroll. Control HB Postings. Coordinate with ACC and PMO on accuracy of postings. Ex post control of payments. European Commission Management costs for payroll services render red	Monthly. Grading Committee (2-3 sessions p.a.)	4,520,000
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	100 000
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	474,200

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	44 000
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	159 000

5.4 ICT

The ICT Section administers the internal ICT systems and networks of the Agency. The ICT Section is an added value entity that relies on servicing client requests and it ensures the planning and good operation of all systems available at all times, including servers, databases, client devices (desktops, laptops, cell phones etc.), area networks, communications etc. Part of the ICT work is entrusted to third parties, especially with regard to IP connections, financial management systems etc., while the ICT Section plays a liaising and support role. The ICT Section is the single point of contact for all IT resources available, responding to user requirements, contingency planning and business continuity. In 2010 the priorities of the ICT Section include:

- Updates in hardware and software that reaches end of life
- Service levels for existing electronic workflows
- Risk management in terms of business continuity

In 2010 the main activities planned are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
4.1	Planning of ICT systems in terms of hardware, software and networks	ICT Networks and Systems in place managed by ENISA or a third party Software license administration User requirements	Systems' availability and integrity. Downtime. Outage Planning	Ongoing	105 000
4.2	ICT Services and ABAC costs	Determine and maintain level of services available	Service delivered according to pre-defined levels	Ongoing	85 000
4.3	Internal ICT Support	ABAC administration and support. General Systems and Networks support and Help Desk. Maintenance. Testing	Calls for assistance. Results of a Test Plan Maintenance plan	Ongoing	0
4.4	Risk Management and Security plan for Agency resources Business Continuity	Management of systems' confidentiality and integrity. Coordinate with ITMAC, the Risk Management Section and the Technical Cabinet	Planning and implementation of risk mitigation measures Handling security incidents	Quarterly	0

5.5 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 plays a dual role in order to ensure the Agency's 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 2010 the priorities of the Legal Section include:

- Back office organisation in terms of an electronic workflow for procurement administration
- Efficient procurement project planning
- Contract management planning

The main activities planned for 2010 are the following:

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
5.1	Legal Advice, as requested by the ED and Departments. Data Protection 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
5.2	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
5.3	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
5.4	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
5.5	Representation	Representation in terms of formal events, and representation before Administrative and Budget Authorities and Courts as authorised by ED.	Number of cases handled	On going	0

5.6 Accounting[13]

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

- Annual accounts of the Agency
- Accounting ledgers that include a journal, a general ledger and an inventory
- Property inventories
- Payments etc.

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
6.1	Payments and Accounts	Carrying out payments Reporting Annual accounts	Accuracy, timely responses, respect of formal deadlines	Ongoing	0
6.2	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

[13] Accounting now reports into the Administration Department as a result of the recent organisational re-alignment.

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	1.6	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	N/A	N/A	13.4	NO
ADA 1.6	Office services	Title 2 excluding Chapter 23 ICT	384 000	10	NO
ADA 1.7	Contacts with and advice on Hellenic Republic Authorities	N/A	N/A	3.2	NO
ADA 1.8	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	3.2	NO
	TOTAL		**384 000**	**38.4**	

ADA 2	Finance	Budget line	Budget	Man months	New Activity
ADA 2.1	Opening and closing of annual budget	N/A	N/A	3	NO
ADA 2.2	Implementation and consolidation of internal controls	N/A	N/A	19.2	NO
ADA 2.3	Annual budget reports	N/A	N/A	2.6	NO
ADA 2.4	Organising carryovers	N/A	N/A	2	NO
ADA 2.5	Payroll administration	N/A	N/A	2	NO
	TOTAL			**28.8**	

ADA 3	Human Resources	Budget line	Budget	Man months	New Activity
ADA 3.1	Staff policy plan	N/A	N/A	2	NO
ADA 3.2	Payroll administration, individual rights & grading	Chapter 11	4 520 000	9.6	NO
ADA 3.3	Performance evaluation	N/A	N/A	4.0	NO
ADA 3.4	Annual training programme	1320	100 000	4	NO
ADA 3.5	Recruitment plan	Chapter 12	474 200	14.6	NO
ADA 3.6	Health and safety at work	1310	44 000	1	NO
ADA 3.7	Third party services	Chapter 14	159 000	0	NO
	TOTAL		**5 297 200**	**38.4**	

ADA 4	ICT	Budget line	Budget	Man months	New Activity
ADA 4.1	ICT systems planning	2300	105 000	4.8	NO
ADA 4.2	ICT services	2301+2302	85 000	4.8	NO
ADA 4.3	Internal ICT Support	N/A	0	14.4	NO
ADA 4.4	IT risk management and Business continuity	N/A	0	4.8	NO
	TOTAL		**190.000**	**28.8**	

Summary of Administration Activities (continued)

ADA 5	Legal and procurement	Budget line	Budget	Man months	New Activity
ADA 5.1	Legal advice and representation	N/A	N/A	6	NO
ADA 5.2	Public procurement	N/A	N/A	9.6	NO
ADA 5.3	Contract management	N/A	N/A	2	NO
ADA 5.4	Operational support	N/A	N/A	0.6	NO
ADA 5.5	Representation	N/A	N/A	1	NO
	TOTAL		**0**	**19.2**	
ADA 6	**Accounting**	**Budget line**	**Budget**	**Man months**	**New Activity**
ADA 6.1	Payments and Annual Accounts preparation	N/A	N/A	25.6	NO
ADA 6.2	Coordination of Audits	N/A	N/A	TBD	NO
	TOTAL		**0**	**25.6**	
	GRAND TOTAL		**5 871 200**	**179.2**	

6 DIRECTORATE ACTIVITIES

At ENISA's Directorate, the reporting lines ensure the horizontal function of Accounting.

6.1 Relations with authorities of the Hellenic Republic

Relations with Hellenic Republic Authorities are associated with the obligation of the Parties to the Seat Agreement signed between the Hellenic Republic and ENISA. The main tasks of this work item concern regular cooperation and interaction with:

- The ministry of Transport and Telecommunication being the competent ministry for information security and the leading ministry in all ENISA matters.
- The designated policy and public administration entities in Greece
- The intra-ministerial committee established by the Hellenic Republic in order to address the emerging ENISA issues rapidly and effectively.
- The local authorities (prefecture, municipality, police) in order to ensure unhindered functioning of the agency and protection of the rights of staff.
- The ministry of Foreign Affairs for managing issues related to the privileges attributed to the agency as a diplomatic mission and its staff (special ID cards, CD plates, VAT exemption etc).

Ref.	Details	Deliverables	Performance Indicators	Deadlines	Budget
6.1.1	Contacts with Hellenic Republic Authorities	Contacting, reporting and following up on the various activities concerning authorities of the Hellenic Republic	Timely handling of each case, respect of deadlines	Ongoing	0

Summary of Administration Activities (continued)

DIR		Budget line	Budget	Man months	New Activity
DIR 1.1	Contacts with and advice on Hellenic Republic Authorities and handling of the Agency's requests pertaining to the implementation of the Seat Agreement.	N/A	N/A	3.2	NO
	TOTAL		**0**	**3.2**	
	GRAND TOTAL		**0**	**3.2**	

7 ANNEX 1 – OPERATIONAL ACTIVITIES 2010

Operational activities 2010	Operational HR (Note 1)	Salary costs Operational HR (Note 2)	Operational Expenditure (Note 3)	Overheads (Note 4)	Total Activity Cost
MTP 1: Improving Resilience in European eCommunication networks	6,2	620.814	545.000	268.396	1.434.210
MTP 2: Developing and maintaining cooperation models	6,3	625.707	315.000	270.512	1.211.218
MTP 3: Identifying emerging risks for creating trust and confidence	3,9	387.813	235.000	167.663	790.476
PA 1: Identify, accountability and Trust in the Future Internet	1,9	187.400	0	81.018	268.418
PA 2: Identifying Drivers and Frameworks for EU Sectoral NIS Cooperation	1,0	101.508	105.000	43.885	250.393
HA 1: Providing advice and assistance	0,0	0	0	0	0
HA 2: Communication and outreach	7,6	759.385	174.000	328.305	1.261.690
HA 3: Managing ENISA bodies and groups	1,6	156.166	210.000	67.515	433.682
HA 4: Managing relations with external stakeholders	0,3	27.069	428.000	11.703	466.772
HA 5: Managing ENISA internal capabilities	0,0	0	45.000	0	45.000
HA 6: Managing ENISA internal communication	0,3	26.028	0	11.253	37.280
HA 7: Work Programme Development	0,9	92.659	0	40.059	132.718
Management activities Sections	4,2	421.129	0	182.066	603.195
Management activities Head of Department	0,9	93.700	0	40.509	134.209
Secretariat activities	6,0	599.679	0	259.259	858.938
Total	**41,0**	**4.099.056**	**2.057.000**	**1.772.144**	**7.928.200**

Note 1 – Operational Human Resources comprise of ENISA Staff and SNEs directly involved in operational activities

Note 2 – Salary costs of Operational Human Resources comprise of the cost of Staff and SNEs directly involved in operational activities

Note 3 – Operational expenditure is the direct cost attributed to each activity, provided for in WP and the Statement of Expenditure 2010

Note 4 – Overhaesd include all non-operational costs, such as salaries of non-operational staff, runni9ng costs (e.g. Office supplies) etc.