# REPUBLIC OF TURKEY

## Ministry of Transport, Maritime Affairs and Communications

# National Cyber Security Strategy
# and
# 2013-2014 Action Plan

[The page intentionally left blank.]

# CONTENTS

[The page intentionally left blank.]

# 1 Introduction

In Turkey, the use of information and communication technologies (ICTs) has been spreading rapidly and ICTs are playing important roles in all aspects of our lives. In addition to public sector organizations, organizations which provide services in critical infrastructure sectors like energy, water resources, health, transportation, communication and financial services have also been heavily using information and communication systems. These systems improve the quality and the speed of the services being provided, thus helping organizations work more productively, contributing to the improvement of living standards.

As our public sector organizations use ICTs to provide services at an increased rate, it has become an important aspect of our national security and competitiveness to ensure the security of information and communication technologies. The vulnerabilities inherent in ICTs may cause denial of service or abuse of service attacks, resulting in potential loss of lives, high scale economic losses, disturbance of public order and/or threats to national security.

It is a fact that cyber space offers opportunities of anonymity and deniability for attacks on information systems and data. The tools and knowledge required for attacks are often cheap and easy to get, and it has been observed that anyone or any systems across the world can participate in cyber-attacks, either knowingly or unknowingly. And it is deemed almost impossible to determine who finances and organizes these enduring and advanced cyber-attacks that target the

information systems and data of critical infrastructures. These facts and conditions reveal the asymmetrical nature of the risks and threats in cyber space, making them even more difficult to tackle.

In light of this context, the Decision made by the Council of Ministers on the "Execution, Management and Coordination of National Cyber Security Activities" was published in the Official Gazette dated 20th October 2012, numbered 28447 and came into force. Pursuant to this cabinet decision;

> *"In order to determine the precautions to be taken for cyber security, to approve - and to ensure implementation and coordination of - the plans, schedules, reports, procedures, principles and standards that have been prepared, a Cyber Security Council has been established, which is to be presided by the Minister of Transport, Maritime Affairs and Communications and which is to consist of the undersecretaries of the Ministries of Foreign Affairs, Interior, National Defense, Transport, Maritime Affairs and Communications, including the undersecretaries of Public Order and Security, National Intelligence Organization, Head of Communication, Electronic and Information Systems of Turkish General Staff, Head of Information And Communication Technologies Authority, Head of The - Scientific And Technological Research Council, Head of Financial Crimes Investigation Council, Telecommunications Communication Presidency and the top managers of the ministries and the public*

*organizations that are to be determined by the Minister of Transport, Maritime Affairs and Communications."*

The cabinet decision has also assigned to the Ministry of Transport, Maritime Affairs and Communications the duty to prepare policies, strategies and action plans on ensuring cyber security at the national level. All public organizations and agencies, natural and legal persons, are obliged to perform the duties assigned in the framework of the policies, strategies and action plans determined by the Cyber Security Council, and to comply with the procedures, principles and standards that were also determined by the Council.

The action plan which was prepared pursuant to this decision defines the activities intended to be carried out within the term 2013-2014, and it also includes the periodical activities beyond these terms as well as the activities that should always be carried out such as training and awareness-raising activities.

### 1.1 Definitions

The concepts used in this document, refer to the following meanings;

**Information systems:** The systems involved in providing services, processes and data by means of information and communication technologies.

**Cyber space:** The environment which consists of information systems that span across the world including the networks that interconnect these systems,

**Information systems of public organizations:** The information systems which belong to and/or are operated by the public organizations and agencies of the Turkish Republic,

**Information systems of natural and legal persons**: The information systems which belong to and/or are operated by the natural and legal persons, subjected to the laws of the Turkish Republic.

**National cyber space**: The environment which consists of the information systems that belong to public organizations, natural and legal persons,

**Confidentiality:** Information systems and data can be accessed by authorized persons or systems only, and the confidential information pertaining to information systems or confidential information in the system will not be disclosed by unauthorized persons or systems.

**Integrity:** Information systems and information can be changed by authorized persons or systems only,

**Accessibility:** Authorized persons and transactions can access information systems and the information therein within the required time and quality,

**Critical infrastructures:** The infrastructures which host the information systems that can cause,

- Loss of lives,
- Large scale economic damages,
- Security vulnerabilities and disturbance of public order at national level

when the confidentiality, integrity or accessibility of the information they process is compromised,

**Cyber security incident:** Violation of confidentiality, integrity or accessibility of information systems or of the information being processed by these systems,

**Cyber security:** Protection of information systems that make up the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information being processed in this space, detection of attacks and cyber security incidents, putting into force the countermeasures against these incidents and then putting these systems back to their states previous to the cyber security incident.

**National Cyber Security:** The cyber security of all services, processes and data –and the systems involved in provisioning of these- provided by the information and communication technologies in the national cyber space.

### 1.2 Objective

The objective of National Cyber Security Strategy and 2013-2014 Action Plan is to create an infrastructure towards achieving;

- the cyber security all of services, processes and data –and the systems involved in provisioning of these- provided by the public organizations and agencies using information technologies,
- the cyber security of information systems of critical infrastructures which are operated by both the public and private sectors,
- minimization of the effects of cyber security incidents, determination of strategic cyber security actions to put systems back to their regular operational states as soon as possible following the incidents, and help with better investigation and prosecution of the incident by law enforcement and judicial authorities.

### 1.3 Scope

The National Cyber Security Strategy and 2013-2014 Action Plan includes the information systems of public organizations and the information systems that belong to critical infrastructures operated by both the public and private sectors.

### 1.4 Update

National Cyber Security Strategy and 2013-2014 Action Plan will be updated at least once a year in a coordinated way at national level, taking into account the

requests from the public and private sectors, and considering also the changing conditions and needs.

## 2 Cyber Security Risks

The risks related to cyber security should realistically be determined in order for the strategic cyber-security actions to be determined in the best way. With the current know-how, the primary risk elements related to ICT systems in Turkey are listed below;

1. The threat is asymmetrical as cyber space provides opportunities of anonymity and deniability for attacks on information systems and data, and the tools and knowledge required for attacks are often cheap and easy to get, and anyone or any systems across the world can participate in cyber-attacks, either knowingly or unknowingly.

2. Any information system can harm another due to the structure of the cyber space that is open to integrated and uninterrupted communication and due to the malware and other similar threat agents existing in the cyber space.

3. Most of the critical services to the populations today are provided and managed by information systems.

4. Most of the information systems of critical infrastructures are accessible through the Internet,

5. There is a lack of national awareness on the subject, in spite of the fact that cyber security at the national level can only be maintained by the contribution of all the citizens,

6. Lack of coordination amongst the partner organizations at the national level in the field of cyber security.

7. Attacks in cyber space to individuals or public agencies go unreported due to the fear of damage to reputation or due to other reasons.

8. The lack of national and international regulations about investigation and prosecution of cyber security incidents makes it even more difficult to cooperate,

9. The services of critical infrastructures are negatively affected not only by cyber-attacks but also by potential errors inherent in information systems, user errors or natural disasters, and there is a lack of capabilities necessary to take measures against these kinds of incidents,

10. Public organizations do not have good enough information security management infrastructures,

11. Public organizations and individuals do not have sufficient level of information and awareness in terms of cyber security,

12. Top managers of public organizations do not have sufficient information about cyber security or they do not seem to be sufficiently interested in the issue of cyber security,

13. Public organizations are not sufficiently structured towards achieving cyber security, and the issue of cyber security is regarded as a responsibility of the IT departments only.

14. The staff in IT departments do not have sufficient level of information and experience in the field of cyber security,
15. There is limited number of staff who would be competent in investigation and prosecution of crimes that have emerged as a result of cyber security violations,
16. The auditing steps about cyber security are not included sufficiently in the internal audit procedures of organizations,
17. Cyber security is not considered as an indispensable component of the information systems which are procured or developed, thus cyber security is not taken into account at sufficient level during procurement of products and services in the area of information and communication technologies in public organizations,
18. There is not enough national manufacturing in terms of hardware and software.

## 3 Principles

The principles to be considered in ensuring national cyber security are as follows:

1. Cyber security should be ensured by methods which are based on risk management and continual improvement.

2. For cyber security, in addition to the technical dimension, an integrated approach should be adopted that would involve determining strong and weak sides in legal, administrative, economic, political and social dimensions, including threats and opportunities.

3. Risk management should be based on the elements of removing technical vulnerabilities, preventing attacks and threats, and minimizing the potential damages.

4. It should be regarded essential that individuals, organizations, societies and governments should perform all their legal and social responsibilities towards achieving cyber security.

5. Full cooperation with the private sector, including the participation into decision-making mechanisms, should be maintained for ensuring the security of critical infrastructures,

6. It is regarded as essential that cooperation should be made with the public and private sectors, universities and non-governmental organizations,

furthermore, international cooperation and information sharing should be ensured in achieving and maintaining cyber space security.

7. It is regarded as essential that diplomatic, technical and law enforcement communication channels should be used continually and effectively for international cooperation and information sharing.

8. International agreements and regulations should be taken into account while the needed legislative actions are carried out.

9. The principles of rule of law, fundamental human rights and freedoms and protection of privacy should be accepted as essential principles.

10. Transparency, accountability, ethical values and freedom of speech should be supported in cyber space.

11. A balance should be kept between security and usability.

12. Auditing and regulatory organizations should take care of ensuring cyber security in areas which they are responsible for.

13. Use of national products and services should be encouraged in meeting the requirements of cyber security, and research and development projects should be endorsed for developing these, and the concept of innovation should be regarded as essential.

## 4 Strategic Cyber Security Actions

Overcoming the threats in cyber space which have been increasing every day and minimizing the vulnerabilities within the national cyber space as much as possible are of utmost importance for progressing towards an information society which we have aimed to reach as a nation. Effective, high quality and affordable usage of information technologies by all the members of the public is important while evolving into an information society, but it is also very important to achieve cyber security during the usage of these information technologies. Therefore, cyber security, which is expressed as the protection of information systems as well as the confidentiality, integrity and accessibility of the information being processed by these systems, is a strategic and multi-stake-holder issue that would affect many aspects such as peace and welfare of the society, the economic development and stability of the nation and the national security of our country which has the aim to become an information society.

In this framework, it has been determined to perform strategic actions towards achieving national cyber security in the 2013-2014 term, in light of the principles determined above. These actions include sub-actions as required, which are listed in the next chapter with the scheduled deadlines and the responsible/relevant organizations. The strategic actions scheduled to be performed in the term 2013-2014 has been grouped under the following titles.

.

**a) Regulatory measures**

In the 2013-2014 term, the government will start to implement regulatory measures, aiming to define the duties, powers and responsibilities of the public organizations and agencies and to remove the existing problems in achieving national cyber security. These actions will be of a nature to support criminal law, civil law, administrative law and the regulation of all procedural provisions thereto. Also, a dictionary on terms of cyber security is to be prepared to prevent potential conceptual confusions.

**b) Activities to help with judicial processes**

Regarding cyber-attacks, in the framework of the international legal requirements, the following should be determined to protect the rights of victims; the source of attack, attacking systems and the severity of effect on the end users who receive service from these systems. In order to produce this information, the national cyberspace should be equipped with reliable recording mechanisms that are compatible with the current technology.

**c) Establishing the National Cyber Incidents Response Organization**

In the short term, a Cyber Incidents Response Organization that will efficiently operate both nationally and internationally is to be created to quickly determine the threats emerging in cyber space, to develop – and to share- precautions for reducing or removing the effects of potential incidents- thus public organizations and agencies will gain the capability to respond to

cyber security incidents. “The National Center for Cyber Incident Response” (USOM), which will be available 7/24 to respond to the threats that may affect the country, will be established, and sectoral "Teams for Responding to Cyber Incidents" (SOME) will be established which are to work under the coordination of the USOM. The sectoral SOMEs will respond to cyber incidents and they will also provide information and hold awareness raising activities specific to the SOMEs affiliated to themselves and to the sector which they are responsible for. Also other SOMEs will be established within public organizations and agencies which are to operate under the coordination of sectoral SOMEs. The USOMs and the SOMEs –while responding to incidents - will also act in coordination with judicial authorities and law enforcement agencies to provide the data that will support the investigation. As the national contact point, the USOM will be in close cooperation with the equivalent authorities of other countries and international organizations.

**d) Strengthening the National Cyber Security Infrastructure**

In the short and the medium term, all public organizations will have wide ranging infrastructure projects that will support the cyber security of public information systems. Activities will be held for ensuring cyber security of public organizations, with priority given to information systems of critical infrastructures. The information systems of key infrastructures, their level of criticality, their relations with one another and the responsible staff will be

determined. The cyber security of the information systems of critical infrastructures will be ensured by both technological precautions and administrative measures and processes. To this effect, the proficiency levels of all staff -on cyber security- primarily those of the top managers in public organizations will be increased through trainings with administrative and technological contents. The public organizations which do not have sufficient proficiency in achieving cyber security will be supported with services to be provided in technological and administrative aspects.

**e) Human Resources Education and Awareness Raising Activities in the Field of Cyber Security**

In the short and medium term, activities will be carried out to create proficient human resources in needed numbers in the field of cyber security. Regulations will be created to include the concept of cyber security into the curricula of primary schools, secondary schools, high schools, non-formal education institutions and higher education organizations. Events will be organized with an aim to raise awareness –on cyber security- of information system auditors, technology developers, system administrators and all other relevant parties, and to provide information that falls under their responsibilities. Auditing steps on cyber security in the internal audit processes of organizations will also be discussed. Also, an education platform will be created for all citizens in order to create and develop

awareness on cyber security, and initiatives serving this purpose will be supported.

**f) Developing National Technologies in the field of Cyber Security**

In the medium and long term, technical know-how and the potential and capabilities of the country on cyber security will be increased. Efforts will be made to have public and private sector work cooperatively in activities towards meeting the needs of research and development.

**g) Extending the Scope of National Cyber Security Mechanisms**

It is necessary to start working on extending the area of responsibility of our national security organizations, to include defense against malicious activities carried out in national and international cyber space.

## 5 National Cyber Security Action Plan for the Term 2013 -2014

This chapter includes the actions towards achieving national cyber security in light of the determined principles for the term 2013-2014 in the framework of the national cyber security strategy. The actions are grouped by the titles determined in the fourth part of this document. One responsible public organization and agency is appointed for each action, however, that action can have more than one relevant organization and agency. In such cases, it is envisioned that all the relevant organizations and agencies should act under the coordination of the responsible organization and agency as required, and should also act in parallel with each other as required, to carry out the activities required by the action. The deadlines for some of the actions are determined, and those actions which are envisioned to be repeated periodically and carried out constantly are particularly specified. There are a total of 29 action items scheduled to take place in 2013-2014.

## 5.1 Carrying out Legislative Activities

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 1. | **Cyber Security Council's start off** | - Cyber Security Council starts off and its operational procedures and principles are determined | Completed | - Ministry of Transport, Maritime Affairs and Communications(Res) |
| 2. | **Establishing the regulations related to cyber security** | - Examining national and international regulations on cyber security and determining the regulations needed | July 2013 | - Ministry of Justice(Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- Ministry of Foreign Affairs(Rel)<br>- Ministry of Interior(Rel)<br>- Ministry of National Defense (Rel)<br>- The undersecretariat of Public Order and Security(Rel)<br>- The Information and Communication Technologies Authority(Rel) |
| | | - Creating a dictionary of cyber security terms | December 2014 | - Turkish Language Association(Res) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 2. | **Establishing the regulations related to cyber security** | - Updating the current main regulations (laws) in a way to cover the subjects that need to be handled in the area of cyber security, and completing the primary legislative activities that would meet the needs for new regulations, and submitting them to the Cyber Security Council. | September 2013 | - Ministry of Justice(Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- Ministry of Foreign Affairs(Rel)<br>- Ministry of Interior(Rel)<br>- Ministry of National Defense (Rel)<br>- Chief of Staff(Rel)<br>- The undersecretariat of Public Order and Security(Rel)<br>- The Information and Communication Technologies Authority(Rel) |
| | | - Carrying out the secondary legislative activities (regulations, edicts, activities related to Cyber Security Services.) | Continually | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The public organizations responsible for regulating and auditing the critical sectors(Rel) |

## 5.2 Carrying Out the Activities That Will Help with Judicial Processes

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 3. | **Improving the evidence base for cyber incidents** | - Determining the minimum requirements for logs to be kept to get reliable evidence for post-incident examination. | June 2013 | - Ministry of Interior(Res)<br>- The Turkish Gendarmerie(Rel)<br>- The undersecretariat of National Intelligence Organization(Rel)<br>- The Turkish National Police (Rel)<br>- The Information and Communication Technologies Authority/ Telecommunications Communication Presidency(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |
| | | - Relevant public organizations put into operation their convenient logging mechanisms in conformity with the current technology and the international standards to get reliable evidence for post-incident examination. | March 2014 | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- Ministry of Interior(Rel)<br>- Ministry of Justice(Rel)<br>- All public organizations(Rel) |
| | | - Public agencies that operate in critical sectors will put into operation their convenient logging mechanisms in conformity with current technology and international standards to get reliable evidence for post-incident examination. | May 2014 | - The public organizations responsible for regulating and auditing the key sectors(Res) |

## 5.3 Creating the National Cyber Incidents Response Organization

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) organizations |
|---|---|---|---|---|
| 4. | **Establishing the National Cyber Incidents Response (USOM) team and establishing the Teams for Responding to Cyber Incidents against Sectoral and Public Entities (SOME)** | - Establishing the National Center for Cyber Incident Response (USOM) which will provide service 24/7. | Completed. | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- Ministry of Interior(Rel)<br>- The Information and Communication Technologies Authority/ Telecommunications Communication Presidency(Rel)<br>- The Turkish National Police (Rel)<br>- The Turkish Gendarmerie(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |
| | | - Preparing the procedures and processes related to the working procedures and principles of the Center to be put into operation for cases that would require national and international cooperation<br>- Preparing a central help page for the public servants working in the area of cyber security and helping them with the online communication of issues to be urgently taken action for. | July 2013 | |
| | | - Preparing the working principles, guidance documents and training schedules to establish and operate the Teams for Responding to Cyber Incidents against Sectoral and Public Entities (SOME) | August 2013 | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The Information and Communication Technologies Authority/ Telecommunications Communication Presidency(Rel)<br>- The public organizations responsible for regulating and auditing the critical sectors(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) organizations |
|---|---|---|---|---|
| 4. | **Establishing the National Cyber Incidents Response (USOM) team and establishing the Teams for Responding to Cyber Incidents against Sectoral and Public Entities (SOME)** | - Establishing the sectoral SOMEs which are specific to critical infrastructure sectors, and creating their teams as well as providing trainings for them. | December 2013 | - USOM (The National Center for Cyber Incident Response) (Res)<br>- The public organizations responsible for regulating and auditing the critical sectors(Rel) |
| | | - Sectoral SOMEs will operate directly under the coordination of USOM<br>- Sectoral SOMEs will benefit from the support to be provided by the USOM | March 2014 | - USOM (The National Center for Cyber Incident Response) (Res)<br>- The public organizations responsible for regulating and auditing the critical sectors(Rel) |
| | | - Establishing the SOMEs of public organizations | September 2014 | - USOM (The National Center for Cyber Incident Response) (Res)<br>- All public organizations(Rel) |
| | | - Public SOMEs will operate directly under the coordination of USOM.<br>- Public SOMEs will benefit from the support to be provided by the sectoral SOMEs and USOM they are affiliated to, if there is any. | December 2014 | - USOM (The National Center for Cyber Incident Response) (Res)<br>- The public organizations responsible for regulating and auditing the critical sectors(Rel)<br>- All public organizations(Rel) |

## 5.4 Strengthening the National Cyber Security Infrastructure

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 5. | **Information security management program in critical infrastructures** | - Determining the critical infrastructures that could be the direct target of cyber threats and that can disturb the public order if damaged. | July 2013 | - The Scientific And Technological Research Council of Turkey (Res)<br>- The public organizations responsible for regulating and auditing the critical sectors(Rel) |
| | | - Conducting the sectoral risk analysis of one of the "critical infrastructures" which is to be determined later on. | August 2013 | |
| | | - Determining the methods of sectoral risk analysis | September 2013 | - The public organizations responsible for regulating and auditing the critical sectors(Res)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- USOM (The National Center for Cyber Incident Response) (Rel) |
| | | - Determining the requirements of sectoral emergency action plans | February 2014 | |
| | | - Completing the first one of the yearly risk analysis reporting activities | March 2014 | |
| | | - Determining and implementing the requirements of sectoral business continuity plans | March 2014 | |
| | | - Determining and implementing the sectoral security precautions | Continually | |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 6. | **Information security program for the public sector** | - Preparing the document on the Minimum Security Requirements to be complied with by public organizations. | August 2013 | - The Scientific And Technological Research Council of Turkey (Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- USOM (The National Center for Cyber Incident Response) (Rel) |
| | | - Providing the first one of the cyber security trainings to the system administrators and to other relevant technical staff based on the priority needs, and determining the proficiency of the trained staff. | The first one was completed | |
| | | - Conducting the first one of the yearly tests and audits which is to be compulsory for public organizations. And for the public organizations which are to be prioritized, these tests and audits will be conducted in agreement with the relevant public organizations. | December 2013 | |
| | | - Publishing and updating the hardening documents and the standards on information systems security | Continually | - The Scientific And Technological Research Council of Turkey (Res) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 7. | **Strengthening cyber security training infrastructure** | - Briefing top managers who are responsible for information systems and cyber security of public organizations | Completed | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- State Personnel Administration(Rel) |
| | | - Training and certifying the technical staff.<br>- Providing trainings to the internal audit staff working in public organizations and agencies, which will help them obtain the competency to carry out audits on information systems. | May 2014 | |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 8. | **Organizing cyber security exercises** | - Organizing cyber security exercises. | To be held once every two years as of 2013. | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- Ministry of Interior(Rel)<br>- The Information and Communication Technologies Authority(Rel)<br>- The Turkish National Police (Rel)<br>- The Turkish Gendarmerie(Rel)<br>- Chief of Staff(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- USOM (The National Center for Cyber Incident Response) (Rel)<br>- Sectoral SOMEs (The Teams for Responding to Cyber Incidents) (Rel) |
| | | - Organizing the first one of the International Cyber Security Exercises with the leadership of Turkey. | May 2014 | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- Ministry of Foreign Affairs(Rel)<br>- The Information and Communication Technologies Authority(Rel)<br>- The Turkish National Police (Rel)<br>- Chief of Staff(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 9. | **Determining the secure communication rules for the public sector** | - Determining the rules and procedures that will help with secure data sharing amongst public organizations | December 2013 | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The National Center for Cyber Incident Response) (Rel)<br>- The Information and Communication Technologies Authority(Rel)<br>- The undersecretariat of Public Order and Security(Rel)<br>- The Scientific And Technological Research Council of Turkey(Rel) |
| 10. | **Implementation of the software security program** | - Preparing the training programs about software security and delivering those programs to software developers | December 2013 | - The Scientific And Technological Research Council of Turkey (Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- Turkish Standards organization(Rel) |
| | | - Publishing the document on fundamental rules on secure software development independent from programming languages for the software to be used in critical infrastructures. | December 2013 | |
| | | - In the scope of the security assessments of the software that have been developed for critical infrastructures; preparing –and submitting to the Cyber Security Council- the feasibility studies towards implementing and checking the technical requirements within critical infrastructure organizations. | March 2014 | |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 11. | **Implementation of cyber threats prevention project** | - Establishing a Honeypot system to detect cyber threats. | July 2013 | - The Information and Communication Technologies Authority/ Telecommunications Communication Presidency(Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |
| | | - Establishing and developing a reporting system for national cyber-attacks. | December 2013 | |
| | | - Generating yearly statistics about cyber threats. | December 2013 | |
| | | - Developing the mechanisms for detection, monitoring and prevention of cyber threats. | December 2014 | |
| 12. | **Certification of products and service providers in the field of cyber security** | - Determining the minimum requirements that natural and legal persons should have, who carry out the security tests on information systems, providing training and consultancy in the field of cyber security, offering the services in other areas to be determined related to cyber security, and designing a certification process for these natural and legal persons. | September 2013 | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- Turkish Standards Organization(Rel) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 12. | **Certification of the products and service providers in the field of cyber security** | - Determining the products of information technology and information systems–including their minimum security requirements- which are used by public organizations and thus are of critical importance, and providing the certification determined. | August 2014 | - Turkish Standards organization(Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- TURKAK (Turkish Accreditation Agency) (Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |
| 13. | **Determining the rules towards issuing a security certification to computer forensics service providers** | - Determining the minimum requirements for natural and legal persons who provide computer forensics services, and designing a certification process for them. | May 2014 | - Ministry of Justice(Res)<br>- Ministry of Interior(Rel)<br>- The Turkish National Police (Rel)<br>- The Turkish Gendarmerie(Rel) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 14. | **Establishing business continuity and data backup systems** | - Determining the security risk levels of the systems – and of the data – which process transactions in electronic environment, regarding all public organizations and agencies and the private sector corporations that run critical information infrastructures. | September 2013 | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- All public organizations and agencies(Rel)<br>- The public organizations responsible for regulating and auditing the critical sectors(Rel) |
| | | - Determining the procedures and principles of backing up sensitive data of all public organizations and agencies and the private sector corporations that run critical information infrastructures. | October 2013 | |
| | | - Preparation of business continuity plans by all public organizations and agencies and the private sector corporations that run critical information infrastructures. | January 2014 | |
| | | - Establishing information systems pursuant to the business continuity plans. | July 2014 | |
| | | - Organizing the exercises suitable for business continuity plans, and submitting the results to the Cyber Security Council. | December 2014 | |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 15. | **Moving the internet web sites of public organizations to local and reliable data centers** | - Determining a public agency or agencies that will offer data center services for storing the internet web sites of public organizations in a domestic and reliable data center. | October 2013 | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The Information and Communication Technologies Authority(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |
| | | - The public organizations like municipalities, hospitals, provincial/district public organizations which do not host their web sites internally will move their web sites to the pre-determined data center/centers. | December 2013 | - All public organizations and agencies (Res) |
| | | - Carrying out regular and periodic inspections of these pre-determined data centers. | Continually | - Ministry of Transport, Maritime Affairs and Communications(Res) |
| 16. | **Developing – and putting into operation- a test infrastructure for detecting data loss** | - Developing an analysis infrastructure that will detect potential data loss from key public organizations. | December 2013 | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The Scientific And Technological Research Council of Turkey (Rel) |
| | | - Determining the public organization on which this test infrastructure will be applied by the Cyber Security Council | January 2014 | |
| | | - Carrying out the tests to detect data loss and reporting the results. | May 2014 | |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 17. | **Determining the levels of access to data in public organizations** | - Creating access control principles in conformity with the international standards (e.g. TS ISO/IEC 27001) | October 2013 | - Cyber Security Council(Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- The Scientific And Technological Research Council Of Turkey (Rel)<br>- All public organizations and agencies (Rel) |
| | | - Re-configuration of e-government applications of public organizations in a way to prevent access to unauthorized data over the internet | February 2014 | |
| 18. | **Promoting the usage of open source products** | - Providing information about existing open source security products that meet the minimum security criteria already determined, which may be used by public and private sector organizations. | October 2013 | - The Scientific And Technological Research Council Of Turkey(Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- Universities (Rel) |
| | | - Creating platforms for developing new cyber security products with open source code. | February 2014 | |
| | | - Preparing a schedule to move the suitable ones -of all the critical information systems- to the operating systems with open source code. | May 2014 | |

## 5.5 Human Resources Education and Awareness-Raising Activities on Cyber Security

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 19. | **Educate academics in the study of cyber security** | - Providing scholarships to students for masters and doctoral studies on cyber security. | October 2013 | - Council of Higher Education(Res)<br>- Ministry of National Education(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- Universities (Rel) |
| 20. | **Wider adoption of cyber security curricula in universities** | - Establishing a commission in the Council of Higher Education regarding the development of cyber security infrastructure. | Completed | - Council of Higher Education(Res)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- Universities (Rel) |
| | | - Adding courses related to cyber security into the curricula of undergraduate, graduate and doctoral programs of relevant departments. | March 2014 | |
| | | - Preparing more books, magazines, articles and other sources on the subject of cyber security in the Turkish language. | Continually | |
| | | - Opening at least two graduate programs on cyber security. | October 2013 | |
| | | - Opening at least one doctoral program on cyber security. | October 2014 | |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 21. | **Implementing a program to direct students towards cyber security expertise** | - Creating scholarship programs for the students who would like to specialize in cyber security | September 2014 | - Council of Higher Education(Res)<br>- Ministry of National Education(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- Universities (Rel) |
| | | - Organizing summer camps on cyber security. | To be held as of the year 2013 | - The Scientific and Technological Research Council of Turkey (Res) |
| | | - Creating internship programs in cyber security. | September 2014 | - Council of Higher Education(Res) |
| | | - Organizing promotion activities in universities related to cyber security. | Continually | |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 21. | **Implementing a program to direct students towards cyber security expertise** | - Organizing cyber defense competitions amongst universities | To be held every year | - The Scientific And Technological Research Council of Turkey (Rel)<br>- Council of Higher Education(Rel) |
| | | - Organizing video/poster competitions on information security for awareness-raising in the primary, secondary, high school and university categories. | To be held every year | - Ministry of National Education(Res) |
| | | - Experts working in USOMs and SOMEs will be trained and they will gain experience in implementation. | Continually | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- The Information and Communication Technologies Authority(Rel)<br>- USOM (The National Center for Cyber Incident Response) (Rel)<br>- SOMEs (The Teams for Responding to Cyber Incidents) (Rel) |
| | | - Increasing the capacities of the security units which will respond to cyber security incidents, and for training experts and helping the experts gain experience in implementation. | Continually | - Ministry of Interior(Res)<br>- The Scientific And Technological Research Council of Turkey (Rel) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 22. | **Promoting cyber security trainings across primary, secondary, high school and non-formal education platforms.** | - Adding cyber security to the curricula of the departments of computer programming in vocational high schools.<br>- Placing the subject of cyber security into the course programs which are under the field of information technology.<br>- Including the cyber security trainings into the scope of the FATIH project<br>- Open source code products should also be included in information technology trainings | March 2014 | - Ministry of National Education(Res)<br>- The Scientific And Technological Research Council Of Turkey (Rel)<br>- The Information and Communication Technologies Authority(Rel) |
| 23. | **Raising awareness of computer users on cyber security.** | - Carrying out activities to increase the awareness level of computer users on cyber security (seminars, brochures, non-formal education activities, remote education by means of the media and awareness-raising) | Continually | - The Information and Communication Technologies Authority(Res)<br>- Ministry of National Education(Rel)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- Radio and Television Supreme Council (Rel) |
| | | - Raising the awareness level of people on safe internet usage and on “safe internet service”, further developing and spreading the service. | Continually | |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 24. | **Organizing national and international cyber security events** | - Organizing symposiums and conferences that would also discuss the economic, social and legal aspects of cyber security.<br>- Participation in international conferences, meetings, seminars and the exercises related to cyber security. | Continually | - Ministry of Transport, Maritime Affairs and Communications(Res)<br>- Ministry of Foreign Affairs(Rel)<br>- The Information and Communication Technologies Authority(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- All public organizations and agencies(Rel)<br>- Universities (Rel)<br>- NGOs (Rel) |

## 5.6 Developing National Technologies in Cyber Security

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 25. | **Stimulating research and development activities** | - Creating and updating a list of the technologies that would meet the cyber security requirements of the country. | Continually | - The Supreme Council for Science and Technology(Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- Ministry of Science, Industry and Technology(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |
| | | - Inclusion of cyber security as a priority subject into the current promotion systems for projects. | March 2014 | |
| | | - Creating the promotion mechanisms for the national Research and Development activities in the field of software, hardware and similar information technology products related to cyber security. | March 2014 | |
| 26. | **Establishing R&D laboratories in the field of Cyber Security** | - Establishing a laboratory infrastructure that would build capacity to detect malware and their effects on information systems. | September 2013 | - The Scientific And Technological Research Council of Turkey (Res) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 26. | **Establishing R& D laboratories in the field of Cyber Security** | - Creating programs that will encourage and support the establishment of Research and Development laboratories on cyber security in universities. | March 2014 | - Council of Higher Education(Res)<br>- Ministry of Development(Rel)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- Ministry of Science, Industry and Technology(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel) |
| | | - Establishing the first cyber security Research and Development laboratory in universities in the scope of the program. | September 2014 | |
| 27. | **Creating national products and solutions in the field of cyber security** | - Holding regular activities in which the public and private sectors, universities, NGOs and other information security stake holders will participate in.<br>- Participants should cooperate on the following subjects; correct usage of information technology products in the scope of cyber security, technological precautions and requirements, Research and Development requirements, information technology products being developed, administrative precautions and regulations. | October 2013 | - Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- The Information and Communication Technologies Authority(Rel)<br>- The Scientific And Technological Research Council of Turkey (Rel)<br>- Universities (Rel)<br>- NGOs (Rel) |

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 28. | **Promoting national products** | - Creating "promotion mechanisms" for public organizations to prefer in their information and communication systems;<br>a. the products which are developed nationally, are assessed in terms of security and are certified,<br>b. the products which were assessed in terms of security and were certified, in cases where there is not any national product.<br>. | February 2014 | - Ministry of Science, Industry and Technology(Res)<br>- Ministry of Transport, Maritime Affairs and Communications(Rel)<br>- Ministry of Development (Rel)<br>- Ministry of Customs and Trade(Rel)<br>- Ministry of Economy(Rel)<br>- Ministry of Finance(Rel)<br>- Public Procurement Authority(Rel) |

## 5.7 Extending the Scope of the National Security Mechanisms

| No | Action | Sub-Action | Deadline | Responsible(Res) and Relevant (Rel) Organizations |
|---|---|---|---|---|
| 29. | **Integrating national cyber security concepts into the national security context** | - Determining the responsibilities of public organizations in case of cyber security incidents in the cyber space and how to ensure coordination at national level. | March 2014 | - Cyber Security Council(Res)<br>- Ministry of Interior(Rel)<br>- Ministry of National Defense(Rel)<br>- Ministry of Justice(Rel)<br>- General Secretariat of the National Security Council(Rel)<br>- Chief of Staff(Rel)<br>- The undersecretariat of National Intelligence Organization(Rel)<br>- The undersecretariat of Public Order and Security(Rel)<br>- The Turkish National Police (Rel)<br>- The Turkish Gendarmerie (Rel) |
| | | - Determining high priority potential attack scenarios targeting the country, including the effects of these attacks. | March 2014 | |
| | | - Determining priority actions required to be carried out to analyze and improve the status of the mechanisms that would be used in case of potential cyber security incidents . | September 2014 | |

[The page intentionally left blank.]