Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020

Tasks defined by the *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020* shall be implemented and fulfilled in a set time frame in order to reach all the goals and objectives of the *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020* successfully.

Tasks defined by the *Action Plan* shall be fulfilled in deep cooperation and interoperability among the entities relevant within the meaning of the Act no. 181/2014 and other public administration institutions, and shall be coordinated with regards to requirements and needs of the entity responsible for the task.

Main Goals	Code	Tasks	Responsible Entity	Deadline
A. Efficiency and enhancement of all relevant structures, processes, and of cooperation in ensuring cyber security				
Develop an effective cooperation model at the national level among the cyber security actors – CERT and CSIRT teams, etc. and reinforce their existing structures and processes.	**A.1.01**	Develop, in coordination with other entities, a scheme and a detailed model of cooperation in ensuring cyber security.	NSA/NCSC *in cooperation with:* MoI MoFA MoD MoIT Intelligence services	Q3 2015
	A.1.02	Analyze cyber security agenda and based on the analysis, define main national interests and priorities in the cyber security field.	NSA/NCSC *in cooperation with:* MoD MoFA MoIT Intelligence services	Q4 2015
	A.1.03	Carry out technical and non-technical cyber security exercises at the national level.	NSA/NCSC *in cooperation with:* MoD MI Intelligence services	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
Develop a national coordinated incident handling procedure that will set acooperation format, contain a communication matrix, a procedure protocol and define each actor's role.	**A.2.01**	Develop a unified methodology for cyber security incident handling on the basis of the Act on Cyber Security and related regulations.	NSA/NCSC	Q1 2016
	A.2.02	Develop a communication matrix for cyber security authorities (national actors, CII, IIS).	NSA/NCSC	Q2 2015
	A.2.03	Provide description of a safe communication interface, which will enable the NSA to receive XML messages with cyber security incident reports automatically. It will also contain an XML schema description that meets the content of the form for cyber security incident reports, mentioned in the regulation no. 316/2014 Coll., complemented by the other non-obligatory options.	NSA/NCSC	Q2 2015
	A.2.04	Develop a protocol of procedures successfully employed in ensuring cyber security.	NSA/NCSC	Q2 2016
Develop a risk assessment methodology at the state level.	**A.3.01**	Choose a risk and a threat assessment methodology for the cyber security field at the state level.	NSA/NCSC	Q1 2018
	A.3.02	Assess, on a continuous basis, cyber security risks and threats at the state level.	NSA/NCSC	Continuously since Q2 2018

Main Goals	Code	Tasks	Responsible Entity	Deadline
Maintain a consistent approach to the Czech Republic's external positions on cyber security issues that will be coordinated with other departments involved in cyber security.	**A.4.01**	Develop an effective model for sharing information about international activities between the NSA and other relevant bodies.	NSA/NCSC *in cooperation with:* MoFA MoD MoIT MoI OFRI	Q2 2016
	A.4.02	Coordinate and harmonize positions in the EU, the NATO and other international organizations with other departments.	NSA/NCSC *in cooperation with:* MoFA MoD MoIT MoI	Continuously since Q3 2015
Reflect in an appropriate manner the continuous development of cyber threats when preparing or reviewing national strategic and security documents (Security Strategy of the Czech Republic and others).	**A.5.01**	Implement the *Security Strategy of the Czech Republic* with regard to increasing cyber threats, and in case of security environment change, suggest the Strategy's revision.	NSA/NCSC MoI MoFA MoD Office of the Czech Government Intelligence services	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
B. Active international cooperation				
Engage actively in international discussions taking place in the forum, programs and initiatives of the EU, the NATO, the UN, the OSCE, the International Telecommunication Union and other international organizations.	**B.1.01**	Cooperate with the EU during the process of the EU Cybersecurity Strategy implementation.	NSA/NCSC MoIT MoFA MoI	Continuously
	B.1.02	Actively cooperate with the EU, the European Council and its agencies in order to ensure better coherence in the cyber topics within the EU.	NSA/NCSC MoIT MoFA MoI MoD	Continuously
	B.1.03	Cooperate and engage actively in the ENISA activities in the field of information and network security.	NSA/NCSC	Continuously
	B.1.04	Actively engage in development and implementation of the cyber measures in order to increase the trust among states in the cyberspace, or in other initiatives corresponding with the visions and principles defined by the Czech NCSS within the OSCE.	NSA/NCSC *in cooperation with:* MoFA	Continuously
	B.1.05	Cooperate with the allies in the process of implementation of the NATO's cyber defence policy.	NSA/NCSC MoD MI	Continuously
	B.1.06	Support cooperation with the NATO in the field of cyber defence, especially with regard to cyber security incident response and exchange of technical information about threats and vulnerabilities.	NSA/NCSC MoD MoFA MI	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
	B.1.07	Support cooperation with the ITU in the field of cyber security technical standards development and implementation.	NSA/NCSC MoIT CTO	Continuously
	B.1.08	Deepen dialogue, through "cyber diplomacy" of the UN member states, about the norms related to the use of ICT in individual countries in order to decrease common danger, protect important national and international infrastructure and build trust and stability among the nations.	MoFA *in cooperation with* NSA/NCSC	Continuously
	B.1.09	Participate in the CCDCOE through national expertise and capabilities and take part,on a continuous basis, in the centre's research activities.	NSA/NCSC MoD	Continuously
Promote cyber security and inter-state dialogue within the Central European region.	**B.2.01**	Participate in and promote the cooperation within the V4 countries and the Central European Cyber Security Platform (CECSP).	NSA/NCSC *in cooperation with* MoFA MoD	Continuously
	B.2.02	Participate in and promote the cooperation with the national security teams in the Central European and East European regions.	NSA/NCSC MoD	Continuously
Establish and deepen bilateral cooperation with other states.	**B.3.01**	Continue and deepen bilateral cooperation with individual states within the cyber security field.	NSA/NCSC *in cooperation with* MoFA MoD	Continuously
Participate in and organize international exercises.	**B.4.01**	Participate in the creation of scenarios for international cyber security exercises on a regular basis.	NSA/NCSC MoD MoI	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
Participate in and organize international trainings.	**B.5.01**	Participate in and organize international trainings, courses and seminars in the field of cyber security.	NSA/NCSC *in cooperation with:* MoFA MoD MoI Intelligence services	Continuously
Participate in creation of an efficient cooperation model and in confidence building among CERT and CSIRT teams at international level, international organizations and academia.	**B.6.01**	Support creation of international communication and information channels among the CERT/CSIRT teams, international organizations and academic centres.	NSA/NCSC MoD	Continuously
	B.6.02	Actively participate in establishing and utilizing NATO projects on the cyber security incident response management and on sharing of technical information about malware with other NATO nations.	NSA/NCSC MoD	Continuously since Q3 2015
Contribute to fostering an international consensus, within formal and informal structures, on legal regulations and behaviour in cyberspace, safeguarding of open Internet, and human rights and freedoms.	**B.7.01**	Join the international discussion about development and implementation of the international legal norms, including the human rights, in the cyberspace.	NSA/NCSC *in cooperation with:* MoFA	Q3 2015
	B.7.02	Join the international discussion on the topic of Internet Governance.	NSA/NCSC *in cooperation with:* MoFA MoIT MoI	Q2 2015

Main Goals	Code	Tasks	Responsible Entity	Deadline
C. Protection of national CII and IIS				
Pursue a continuous analysis and control of CII and IIS security in the Czech Republic based on a clearly defined protocol.	**C.1.01**	Pursue a continuous identification of the CII and IIS entities that come under the Act on Cyber Security and related regulations.	NSA/NCSC *in cooperation with:* MoI	Continuously
	C.1.02	Provide the CII and IIS entities with consultation, communication and methodical support.	NSA/NCSC	Continuously
	C.1.03	Support and control the CII and IIS entities in the process of legal requirements implementation.	NSA/NCSC	Continuously
	C.1.04	Cooperate with international partners in the assessment of the CII determination, especially in terms of cross-border matters.	NSA/NCSC	Continuously
Support creation of new CERT and CSIRT teams in the Czech Republic.	**C.2.01**	Inform the private entities (especially those that are part of the CII) about CERT and CSIRT teams' advantages, i.e. ensuring better cooperation during the cyber security incident handling, and support its creation.	NSA/NCSC	Continuously
	C.2.02	Support creation of CERT and CSIRT teams within the departments and other state institutions, and also within the industry.	NSA/NCSC	Continuously
	C.2.03	Establish Ministry of Interior's CERT and CSIRT team in order to protect fundamental registers and systems necessary for the proper function of e-Government.	MoI *in cooperation with:* NSA/NCSC	Q1 2016

Main Goals	Code	Tasks	Responsible Entity	Deadline
Enhance, on a continuous basis, the CII and IIS networks' resistance, integrity and trustworthiness.	**C.3.01**	Increase, on a continuous basis, the NCSC's, respectively the GovCERT.CZ's capacities and reflect personal and knowledge requirements emerging from the country's cyber security state development.	NSA/NCSC	Continuously
	C.3.02	Create a recommending cyber security framework for entities outside the CII and the IIS, i.e. the set of standards and proved procedures that can help the organizations to handle cyber security risks.	NSA/NCSC	Q3 2015
	C.3.03	Keep the cyber security incidents register updated, carry out the incident assessments and suggest necessary measures.	NSA/NCSC	Continuously
	C.3.04	Define minimum log requirements that are necessary for reliable cyber security incident ex-post analysis.	NSA/NCSC	Q4 2015
	C.3.05	Develop and implement a honeypot system for cyber threat detection.	NSA/NCSC	Q3 2016
	C.3.06	Map the relationship between the public administration networks and its ISP in order to ensure efficient cooperation during the cyber security incident handling.	NSA/NCSC	Continuously since Q4 2015

Main Goals	Code	Tasks	Responsible Entity	Deadline
	C.3.07	Provide and methodically control deployment of the detection systems for networks operation and cyber security incidents monitoring within the civil service.	NSA/NCSC	Q1 2017
	C.3.08	Establish a laboratory for malware impacts on the information systems detection and testing.	NSA/NCSC	Q2 2016
	C.3.09	Create and develop cyber security incident simulation scenarios and programs that can be used during the national exercises.	NSA/NCSC *in cooperation with:* MoD MoI Intelligence services	Continuously since Q3 2015
	C.3.10	Develop and use capacities and capabilities for carrying out cyber security tests.	NSA/NCSC	Continuously since Q3 2015
	C.3.11	Develop and improve capacities and capabilities for forensic analysis and other supportive services within the cyber security for the Czech Republic's use.	NSA/NCSC	Continuously since Q3 2015
	C.3.12	Support the Fenix project and the public administration networks' involvement in order to keep the service functional during the massive cyber attacks.	NSA/NCSC *in cooperation with:* MoI	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
Analyse and monitor, on a continuous basis, the threats and risks in the Czech Republic.	**C.4.01**	Collect and analyze information about the threats and risks in order to provide an overview of current cyber security state in the Czech Republic and in the world.	NSA/NCSC *in cooperation with:* Intelligence services	Continuously
	C.4.02	Detect the network operation anomalies and identify potential cyber threats.	NSA/NCSC	Q1 2016
	C.4.03	Develop abilities to actively obtain information, in cyberspace, about possible threats and risks for the cyber security of the Czech Republic.	Intelligence services	Continuously
	C.4.04	Analyze content of the information about the threats and risks relevant to the Czech Republic's interests obtained in the cyberspace, including analysis of its effects on the public, and develop a procedure for the effective mutual exchange of information about the threats and risks among relevant actors.	Intelligence services *in cooperation with:* NSA/NCSC	Continuously
	C.4.05	Support coordination during prevention in the cyber security field and obtain information about cyber attacks planning in order to prevent the attack's execution.	SIS OFRI	Continuously
	C.4.06	Modernize and strengthen the number of personnel of the specialized intelligence services units.	SIS OFRI	Continuously since Q1 2016

Main Goals	Code	Tasks	Responsible Entity	Deadline
	C.4.07	Establish and develop cooperation among the Czech intelligence services and among relevant national and international entities.	NSA/NCSC Intelligence services	Continuously
Share, in an efficient manner, information among the state and CII and IIS entities.	**C.5.01**	Make, on a continuous basis, the cyber security threats and incidents warnings together with the risk handling recommendations public.	NSA/NCSC	Continuously
	C.5.02	Develop an automated platform for sharing information about cyber security threats and incidents with the relevant threatened entities on the basis of completed mapping of the elements securing the CII and the IIS.	NSA/NCSC	Q4 2015
	C.5.03	Extend the cyber incidents reports possibilities by web form and communication among the systems.	NSA/NCSC	Q1 2015
	C.5.04	Develop a safe platform for communication during massive incident handling at the national level.	NSA/NCSC	Q4 2015

Main Goals	Code	Tasks	Responsible Entity	Deadline
Continue to increase technological capacities and capabilities of the National Cyber Security Centre (hereinafter "NCSC") and of GovCERT.CZ while providing their personnel with continuous training and education.	**C.6.01**	Provide, on a continuous basis, the NCSC's personnel with education and training in the cyber security field.	NSA/NCSC	Continuously
	C.6.02	Through foreign courses, keep awareness of up-to-date cyber security trends and threats that Czech Republic, as an active EU and NATO member, faces.	NSA/NCSC	Continuously
	C.6.03	Increase the GovCERT.CZ's capabilities to identify cyber security incidents characteristics.	NSA/NCSC	Continuously since Q2 2016
	C.6.04	Establish and spread GovCERT.CZ's early warning detection system.	NSA/NCSC	Q3 2017
	C.6.05	Establish a nonstop emergency service for cyber security incidents monitoring and handling in GovCERT.CZ.	NSA/NCSC	Q1 2016
Secure in a thorough and reliable manner a CII and IIS data storage environment to be established and managed by the state.	**C.7.01**	Develop a National Cloud Computing Strategy and propose it to the government.	MoI *in cooperation with:* MoF NSA/NCSC	Q4 2015

Main Goals	Code	Tasks	Responsible Entity	Deadline
	C.7.02	Prepare a state cloud project, including the data storage and other necessary documents (financial, security, organizational and technical requirements), and propose it to the government.	MoI *in cooperation with:* MoF NSA/NCSC	Q1 2016
	C.7.03	Map the current state and, if needed, prepare the legislative changes proposal with regard to the creation of a state cloud including the data storage.	MoI *in cooperation with:* NSA/NCSC	Q1 2018
Perform regular testing of and detect errors and vulnerabilities in information systems and networks used by the state, based on CII and IIS penetration testing principles.	**C.8.01**	Detect errors and vulnerabilities in the CII and IIS systems and networks using the announced penetration tests.	NSA/NCSC	Q1 2017
Enhance, on a continuous basis, technological and organizational prerequisites for active countering (suppression) of cyber attacks.	**C.9.01**	Establish the National Cyber Forces Centre (NCFC) within the Military Intelligence that will be able to perform a wide range of operations in the cyberspace and other activities necessary for ensuring state's cyber defence. NCFC will be able to perform military operations in the cyberspace, supporting international operations of the Czech Army within the NATO or the EU, or in case of need to defend the Czech Republic in a hybrid conflict.	MI	Continuously since Q1 2016

Main Goals	Code	Tasks	Responsible Entity	Deadline
	C.9.02	Prepare the NCFC funding and development project.	MI	Q4 2015
	C.9.03	Provide the NCFC with a suitable workplace and personnel recruitment.	MI	Continuously since Q4 2015
	C.9.04	Develop complete technical infrastructure for the NCFC.	MI	Continuously since Q1 2016
	C.9.05	Prepare a proposal of legislative changes necessary for the NCFC full functionality.	MI *in cooperation with:* NSA/NCSC SIS OFRI	Q3 2015
Increase national capacities for active cyber defence and cyber attack counter-measures.	**C.10.01**	Fully ensure cyber defence in the Czech Republic by means of cooperation among the NCFC, NCSC and national CERT and other CERT/CSIRT teams.	MI	Q1 2020
	C.10.02	Define a set of possible crisis situations and create scenarios for crisis cooperation, communication and counter-measures deployment during the state of emergency.	NSA/NCSC *in cooperation with:* MoD MI	Continuously since Q3 2015
	C.10.03	Perform national exercises in the field of communication, coordination and cooperation in ensuring cyber defence.	MI *in cooperation with:* NSA/NCSC	Continuously since Q1 2017

Main Goals	Code	Tasks	Responsible Entity	Deadline
Train experts specialised in questions of active counter-measures in cyber security and cyber defence and in offensive approach to cyber security in general.	**C.11.01**	In NCSC, reflect personnel and knowledge requirements emerging from the state of cyber security in the world and share these capabilities and skills with relevant bodies.	NSA/NCSC	Continuously
	C.11.02	In NCFC, reflect personnel and knowledge requirements emerging from the state of cyber defence in the world.	MI	Continuously
Develop a procedure for transition from the state of cyber emergency declared pursuant to the Act on Cyber Security, to the states defined in Constitutional Act No. 110/1998 Coll., on Security of the Czech Republic.	**C.12.01**	Develop a procedure for transition from the state of cyber emergency declared pursuant to the Act on Cyber Security, to the states defined in Constitutional Act No. 110/1998 Coll., on Security of the Czech Republic.	NSA/NCSC *in cooperation with:* MoI MoFA MoD MI Office of the Czech Government	Q1 2016
	C.12.02	Establish a working group consisting of MoD, MoFA, MoI, intelligence services and NSA/NCSC experts on international law in the matter of ensuring cyber security and cyber defence on an international scale.	NSA/NCSC *in cooperation with:* MoI MoFA MoD Intelligence services	Q3 2015

Main Goals	Code	Tasks	Responsible Entity	Deadline
D. Cooperation with private sector				
Continue cooperation with private sector and raise general awareness of the NSA's activities in the cyber security field.	**D.1.01**	Create contact and cooperate with private sector and raise general awareness of the NSA's activities and cooperation possibilities through regular meetings and mutual information sharing.	NSA/NCSC	Continuously
	D.1.02	Work, together with electronic communication and information society services providers, on the unified approach to help the Czech internet users to detect and protect themselves from harmful activities on their systems.	NSA/NCSC	Continuously
Create, in cooperation with private sector, uniform security norms, standardize the cooperation and set an obligatory protection level for CII entities.	**D.2.01**	Create, in cooperation with private entities, requirements for security norms and mandatory protection levels for CII entities.	NSA/NCSC	Continuously
	D.2.02	Support cyber security norms development via national and international standardization and certification authorities and institutions, and support the norms acceptance by the private entities.	NSA/NCSC	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
Ensure, in cooperation with private sector, a cyberspace offering a reliable environment for information sharing, research and development and provide a secure information infrastructure stimulating entrepreneurship in order to support the competitiveness of all Czech companies and protect their investments.	**D.3.01**	Promote high level of cyber security in the public service, thus maximize the private organizations and general public use of e-Government.	MoIT MoI	Continuously
	D.3.02	Coordinate transition from IPv4 protocol to IPv6 protocol and inform about security risks related to the process of transition.	MoIT *in cooperation with:* MoI	Continuously
	D.3.03	Support spreading of DNSSEC for web presentations securing and monitor, on a regular basis, the state of DNSSEC implementation in the public administration and the Czech national domain (.cz).	MoIT	Continuously
Provide education and raise the private sector's awareness of cyber security. Provide the private sector with guidance on how to behave in crisis situations, particularly during cyber incidents but also in their day-to-day activities.	**D.4.01**	Provide the private entities with consultation and organize educational and enlightened activities.	NSA/NCSC	Continuously
	D.4.02	Support small and medium enterprises through the informative cyber security campaign targeting enterprises' needs and possibilities.	NSA/NCSC MoIT	Continuously
Build trust between private sector and the state, including through creation of a national platform/system for information sharing regarding threats, incidents and imminent dangers.	**D.5.01**	Create a platform for sharing the information about cyber threats and vulnerabilities between the NCSC and the CII and IIS entities.	NSA/NCSC	Q1 2016

Main Goals	Code	Tasks	Responsible Entity	Deadline
E. Research and development / Consumer trust				
Participate in national and European research projects and activities concerning cyber security.	**E.1.01**	Map the current state of R&D dealing with cyber security and technologies used in the Czech Republic.	NSA/NCSC *in cooperation with:* MoI MoD	Q1 2018
	E.1.02	Prepare, in cooperation with other state institutions, national concept regarding the R&D in the cyber security field.	NSA/NCSC *in cooperation with:* MoI MoD Czech Police TACR Intelligence services	Q3 2018
	E.1.03	Prepare and fulfil a plan of the NSA's research activities in the cyber security field with regard to state's current and future needs.	NSA/NCSC *in cooperation with:* MoD Intelligence services	Q3 2017

Main Goals	Code	Tasks	Responsible Entity	Deadline
Designate the NSA as the main point of contact for cyber security research. The NSA shall contribute to coordination of research activities in this field in order to avoid duplications. Cyber security research will thus focus on substantive problems and on transfer of research outputs into practice.	**E.2.01**	Create a database of the projects within cyber security and use it to spread the information to other entities.	NSA/NCSC	Q1 2019
	E.2.02	Establish a working group consisting of representatives of all organizations dealing with the R&D within the cyber security field, i.e. mainly the NSA/NCSC, MoI, MoD, TACR and intelligence services.	NSA/NCSC *in cooperation with:* MoI MoD TACR Intelligence services	Q3 2017
Cooperate with private sector and academia on development and implementation of state used technologies in order to ensure their maximum protection and transparency. Test and evaluate the level of security of the technologies used.	**E.3.01**	Initiate the research projects and cooperate with private sector on its implementation.	NSA/NCSC	Continuously
Cooperate with private sector and academia on research projects (including primary and experimental research) and on activities in technical disciplines and social sciences, at the national, as well as European and international, transatlantic levels.	**E.4.01**	Cooperate with academia and private sector on research projects and provide them with necessary information and strategic leadership. Involve the Czech republic and its academia and private sector in research programs at European, international and transatlantic levels.	NSA/NCSC MEYS	Continuously
	E.4.02	Support and participate in academic publication activities regarding the cyber security field.	NSA/NCSC	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
F. Education, awareness raising and information society development				
Raise cyber security awareness and literacy of primary and secondary school students, as well as among the large public, i.e. end users, through the intermediary of supporting initiatives, awareness campaigns, organizing public conferences etc.	**F.1.01**	Support the initiatives and enlightenment campaigns; organize conferences and workshops for the large public, i.e. end users.	NSA/NCSC *in cooperation with:* MoLSA	Continuously
	F.1.02	Run and update, on a continuous basis, the GovCERT.CZ portal as a platform informing the large public about current cyber security threats, risks, vulnerabilities and other NSA activities.	NSA/NCSC	Continuously
	F.1.03	Create an e-learning platform for the large public and expert community education.	NSA/NCSC *in cooperation with:* MoLSA	Q1 2016
Modernize the existing primary and secondary school curricula and support new university study programs designed to produce cyber security experts.	**F.2.01**	Modernize primary and secondary school curricula.	NSA/NCSC MEYS	Q1 2017
	F.2.02	Prepare methodology and materials for schools in order to reach an easy implementation of the cyber security issues in the school education programs according to new framework education programs.	NSA/NCSC MEYS	Q1 2017
	F.2.03	Prepare a sufficient amount of methodical materials for school teachers; provide the teachers with education within the cyber security field and prepare a sufficient amount of school materials for students.	NSA/NCSC MEYS	Q1 2017

Main Goals	Code	Tasks	Responsible Entity	Deadline
	F.2.04	Create an overview of national and international school programs dealing with the cyber security, update it continuously and promote it.	NSA/NCSC	Q4 2015
	F.2.05	Raise awareness about responsible and safe use of Internet, ICT and of new media.	NSA/NCSC *in cooperation with:* MoLSA	Continuously
	F.2.06	Support, in coordination with universities, and develop the students' talent in the cyber security field.	NSA/NCSC	Continuously
	F.2.07	Provide university students with the possibility of internship in the cyber security field in the Czech Republic and also abroad.	NSA/NCSC MoD	Continuously
	F.2.08	Cooperate on creation of new study programs in the cyber security and cyber defence fields and cooperate with universities and colleges on implementation of these new programs, on creation of new curricula, etc.	NSA/NCSC MoD	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
Provide relevant education and training to public administration staff involved, but not exclusively, in the field of cyber security and cybercrime.	**F.3.01**	Train existing public administration personnel in the field of cyber security.	NSA/NCSC MoLSA MoI	Continuously since Q4 2015
	F.3.02	Train cyber security managers in the public administration in the detection (e.g. anomalies detection), cyber security incidents reporting, and in other possibilities of cooperation with the NCSC.	NSA/NCSC MoLSA	Continuously
	F.3.03	Institutionalize other educational programs by getting certificates for passing the study programs.	NSA/NCSC MoLSA MoI	Continuously
	F.3.04	Raise the level of education in the cyber security field using the modern teaching methods.	NSA/NCSC MoLSA	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
G. Support to the Czech Police capabilities for cybercrime investigation and prosecution				
Reinforce the personnel of individual cybercrime police departments.	**G.1.01**	Reinforce the personnel of the Czech Police Presidium's cybercrime department by systematized service positions and systematized working positions that will mitigate existing crisis and provide human potential necessary for the fulfilment of required activities.	Czech Police MoI	By 2018
	G.1.02	Reinforce the personnel of the Organized Crime Detection Unit, Unit for Combating Corruption and Financial Crime, and of the National Anti-Drug Centre with regard to criminal acts investigation related to cybercrime, including the terrorism combating area that overlaps the ICT environment.	Czech Police MoI	By 2018
	G.1.03	Reinforce the personnel of the Criminal Police and Investigation Service's executive departments, which have been appointed as cybercrime departments, by systematized service positions and working service positions in each region. This task responds to the local situation within the regional parts of the Criminal Police and Investigation according to the model respecting the division of each cybercrime department into technical, operative and procedural aspects. It provides mitigation of the existing state, leadership of the difficult criminal proceeding and it ensures action readiness.	Czech Police MoI	By 2018

Main Goals	Code	Tasks	Responsible Entity	Deadline
	G.1.04	Reinforce the personnel of the Police regional expert departments' infrastructure by systematized service positions that will mitigate existing disproportion of provided activities and personnel capacities.	Czech Police MoI	By 2018
	G.1.05	Reinforce the personnel of the Special Activities Unit in the field of programming by systematized service positions, in the field of systems' technical administration by systematized service positions that will be able to accept, analyze and deal with the increasing number of requirements and of the Internet's operation and localization data.	Czech Police MoI	By 2018
	G.1.06	Reinforce the personnel of the Special Activities Unit by systematized service positions to support special activities related to the information technologies penetration to the field of criminal investigation activities.	Czech Police MoI	By 2018
	G.1.07	Reinforce the personnel of the IT operations department that secures technological data administration and IT support.	Czech Police MoI	By 2018
Modernize technological equipment of specialized police departments.	**G.2.01**	Set mandatory and enforceable minimum technology equipment requirements for all cybercrime departments and provide required equipment and technology.	Czech Police MoI	By 2018

Main Goals	Code	Tasks	Responsible Entity	Deadline
	G.2.02	Set mandatory and enforceable minimum technology equipment requirements for the expert departments dealing with the so called computer analysis and provide required equipment and technology.	Czech Police MoI	By 2018
	G.2.03	Jointly coordinate the planning of individual purchases for cybercrime departments and computer analysis expert departments with the guarantee of allocations tied to the budget plans for the next periods.	Czech Police MoI	By 2018
	G.2.04	Gradually decrease the distance between Criminal Police and Investigation expert departments at each level with respect to existing state of departments' deployment.	Czech Police MoI	By 2018
Establish direct and prompt cooperation links for the field of cybercrime between relevant national entities and other security forces.	**G.3.01**	Establish legal ties enabling and guaranteeing direct and prompt cooperation with the security forces (SIS, OFRI, MI) and with the CII entities, the NCSC, GovCERT.CZ and national CERT team within the executive level.	Czech Police MoI *in cooperation with:* MP	Q3 2016
Support international cooperation in information sharing and training in the field of cybercrime.	**G.4.01**	Cooperate with international partners in the field of cybercrime information sharing and education.	Czech Police MoI *in cooperation with:* MP	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
Provide professional education and training to police specialists.	**G.5.01**	Extend the qualification courses by basic knowledge and skills related to cybercrime and establish an electronic, or similar, system of continuous education.	Czech Police MoI	Continuously, by Q2 2017
	G.5.02	Extend the specialized courses for Criminal Police and Investigation's policemen by wider knowledge related to cybercrime.	Czech Police MoI	Continuously, by Q2 2017
	G.5.03	Prepare the courses for police cybercrime experts.	Czech Police MoI	Continuously, by Q2 2017
	G.5.04	Create conditions for continuous education of the Czech Police experts in the field of cybercrime in the commercial and academic sectors.	Czech Police MoI	Continuously, by Q2 2017
	G.5.05	Strengthen and extend conditions for experts' language education by general language courses, expert language courses and language improvement courses, and put emphasis on the language skills in the next recruitments.	Czech Police MoI	Continuously, by 2017
Create a multidisciplinary academic environment to enhance the Czech Police capacities in cybercrime prosecution.	**G.6.01**	Create a multidisciplinary academic environment to enhance the Czech Police and other security entities' capabilities in cybercrime prosecution, and resolve related security, standardization, legislative, research and other needs.	Czech Police MoI	Continuously by 2018

Main Goals	Code	Tasks	Responsible Entity	Deadline
H. Cyber security legislation (development of legislative framework). Participation in creation and implementation of European and international regulations				
Create a comprehensible, effective, and adequate cyber security legislation based on systematic approach and taking into account the existing legislation.	**H.1.01**	Create comprehensible, effective and adequate cyber security legal and sub-legal legislation.	NSA/NCSC *in cooperation with*: MoFA	Continuously
	H.1.02	Analyze the regulations necessary for the effective ensuring cyber security in the Czech Republic.	NSA/NCSC *in cooperation with*: MoFA	Continuously
Participate actively in creation and implementation of European and international regulations.	**H.2.01**	Participate, on a continuous basis, in the development and implementation of European and international legislative framework and rules in the cyber security field.	NSA/NCSC MoFA	Continuously
	H.2.02	Participate in the discussions on the topic of cyber security and cyber defence concepts' relevance.	NSA/NSC MoFA MoD MoI Intelligence services	Continuously

Main Goals	Code	Tasks	Responsible Entity	Deadline
Assess, on a continuous basis, the effectiveness of cyber security legislation and its conformity to the latest findings in relevant technical disciplines and social sciences, and regularly update and amend such legislation in order to reflect current requirements of a secure information society.	**H.3.01**	Regularly update and amend cyber security legislation on the basis of continuous analysis of its effectiveness and conformity with the latest findings in relevant technical disciplines and social sciences.	NSA/NCSC	Continuously
	H.3.02	Set a mandatory level for securing the CII entities by updating the legal and sub-legal legislation.	NSA/NCSC	Continuously
	H.3.03	Revise and create proposal of legislative changes of chosen sections of Criminal Code and of Act on Electronic Communications that would make the cybercrime investigation and prosecution more effective, and that would reflect current situation in the cybercrime field.	MoI Czech Police CTO *in cooperation with:* Intelligence services	Q1 2016
Support cyber security related education of the judiciary (ie. Prosecutors or judges).	**H.4.01**	Provide imposition and enforcement of adequate sanctions in legal disputes related to cyber issues by education of the judges and prosecutors.	NSA/NCSC MoJ MoI Czech Police	Continuously

LIST OF ABBREVIATIONS

CCDCOE – Cooperative Cyber Defence Centre of Excellence

CECSP – Central European Cyber Security Platform

CERT – Computer Emergency Response Team

CII – Critical Information Infrastructure

CSIRT – Computer Security Incident Response Team

CTO – Czech Telecommunication Office

DNSSEC – Domain Name System Security Extensions

ENISA – European Union Agency for Network and Information Security

EU – European Union

ICT – Information and Communication Technologies

IIS – Important Information Systems

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

ISP – internet service provider

ITU – International Telecommunication Union

MEYS – Ministry of Education, Youth and Sport

MI – Military Intelligence

MISP – Malware Information Sharing Platform

MoD – Ministry of Defence

MoF – Ministry of Finance

MoFA – Ministry of Foreign Affairs

MoI – Ministry of the Interior

MoIT – Ministry of Industry and Trade

MoJ – Ministry of Justice

MoLSA – Ministry of Labour and Social Affairs

MP – Military Police

NATO –North Atlantic Treaty Organization

NCFC – National Cyber Forces Centre

NCSS – National Cyber Security Strategy

NSA/NCSC – National Security Authority / National Cyber Security Centre

OFRI – Office for Foreign Relations and Information

OSCE – Organization for Security and Cooperation in Europe

R&D – research and development

SIS – Security Information Service

TACR – Technology Agency of the Czech Republic

V4 – Visegrád Group

XML – Extensible Markup Language