National Security Authority
National Cyber Security Centre

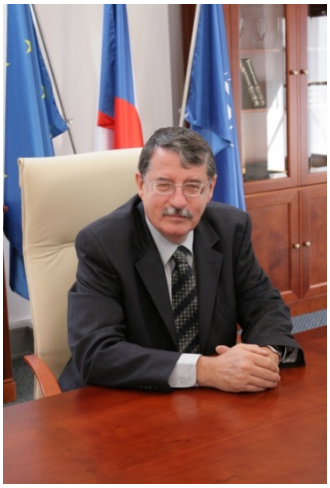
NATIONAL CYBER SECURITY STRATEGY

OF THE CZECH REPUBLIC

FOR THE PERIOD FROM 2015 TO 2020

CONTENT

Foreword



Human actions and activities are increasingly moving from the physical environment to cyberspace. Information and communication technologies have, during the last decade, changed almost every aspect of our lives by significantly facilitating communication or sharing and access to information and services. This phenomenon, however, makes our society more vulnerable and cyber security thus becomes one of the most important challenges that the state must respond to.

Since 2011, the National Security Authority has been operating as the coordinator and national authority in the field of cyber security in the Czech Republic. During that period, we have achieved, inter alia, two important milestones identified by the previous "Cyber Security Strategy of the Czech Republic for the period of 2012 to 2015": adoption of the Act on Cyber Security[1] and opening, in May 2014, of the National Cyber Security Centre including a fully operational Government Computer Emergency Response Team for cyber security incidents handling.

Other objectives set out in the above strategy can also be considered to have been met. The Czech Republic regularly participates in several international cyber security exercises, has successfully launched the mapping of critical information infrastructure and of important information systems, and established cooperation with stakeholders at both the national and international levels. It can therefore be concluded that the previous strategy has been successfully implemented and the level of cyber security in the Czech Republic has significantly increased since 2012. With the approaching expiration of the "Cyber Security Strategy of the Czech Republic for the period of 2012 to 2015" and having fulfilled all main objectives and tasks, the National Security Authority undertook to develop a new "National Cyber Security Strategy for the period from 2015 to 2020" which would constitute a major breakthrough in the Czech Republic's approach to cyber security.

[1] Act on Cyber Security and Change of Related Acts (No. 181/2014 Coll.).

Compared to the previous strategy, we are now moving from the building of basic capacities necessary to guarantee an elementary level of cyber security towards its deeper and enhanced mode of development.

Publishing this new national strategy, we define the Czech Republic's visions and priorities in the field of ensuring cyber security. The Czech Republic will face many cyber security threats and risks in the years to come and our networks and systems must always remain stable and secure. The new strategy therefore determines how to achieve such condition and identifies the ways and tools the Czech Republic shall use to reduce the risks and to mitigate threats arising from cyberspace without any limitation to the benefits derived from its use.

Cyber security cannot be achieved without deep mutual trust and cooperation between the public sector and the rest of the society. Although the National Security Authority of the Czech Republic has become the national authority for cyber security, this does not relieve any public or private entity including individuals of their overall responsibility and role in ensuring cyber security. Only by working together can we create a truly open and secure cyberspace where we all shall prosper.

Dušan Navrátil

Director

Cyber security is continuously gaining on importance and already represents one of the determinative factors of the Czech Republic's security environment. Cyber security comprises a sum of organizational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace in the Czech Republic for the benefit of both public and private sectors, as well as for the general public. Cyber security helps to identify, evaluate, and resolve cyber threats, to reduce cyber risks and to eliminate impacts of cyber attacks, cyber crime, cyber terrorism and cyber espionage by enhancing confidentiality, integrity, and availability of data, information systems and other elements of information and communication infrastructure. The main purpose of cyber security is protection of cyber space to allow the individuals' right to informational self-determination to be realized.

Introduction

Ensuring cyber security of a state constitutes one of the key challenges of the present day. The public and private sectors' dependence on information and communication technologies becomes ever more obvious. Information sharing and protection are crucial for the protection of security and economic interests of the state and its citizens. Whilst the general public is mostly concerned about their personal data abuse or afraid of losing money and data, cyber security as such encompasses much more. Major risks include cyber espionage (industrial, military, political, or other), ever more often carried out directly by governments or their security agencies, organized crime in cyberspace, hacktivism, intentional disinformation campaigns with political or military objectives, and even – in the future – cyber terrorism. Beside cyber attacks, frequently motivated by financial benefit, cyber security can also be compromised by unintended disruptions of network security and integrity due to, for instance, human factor failures or natural disasters.

The state must be able to effectively react to all current and future challenges posed by the always changing threats originating in the dynamically evolving cyberspace, and thereby guarantee the latter's security and reliability.

Due to the open and publicly accessible nature of the Internet characterized by absence of geographical borders, security and protection of cyberspace demand a proactive approach not only from the state, but also from its citizens. Although the state constantly builds and increases relevant national capacities, its efforts will not reach the necessary level of efficiency without cooperation with private sector and academia, nor without intensive international cooperation and, in particular, involvement of individuals.

This National Cyber Security Strategy of the Czech Republic for the period from 2015 – 2020 (hereinafter "Strategy") constitutesa fundamental conceptual document of the Czech Government for the given field, reflecting security interests and principles as defined in the Security Strategy of the Czech Republic.It shall serve as a base document for development of legislation, policies or standards, guidelines, and other recommendations related to cyberspace protection and security.

The Strategy follows the logical framework provided by the Methodology for Public Strategies Development and other relevant recommendations. The document first outlines the Czech Republic's vision of the cyber security field beyond the temporal scope of the Strategy (2015 – 2020) and defines the basic principles followed by the state in view of ensuring its cyber security. The subsequent text identifies concrete challenges in the cyber security field faced by the Czech Republic and international community as a whole of which the Czech Republic forms part. Finally, main strategic goals are presented that must be achieved in order to respond to those challenges and which shall serve as a basis for a detailed Action Plan for the Cyber Security in the Czech Republic for the period from 2015 to 2020 (hereinafter 'Action Plan').

Visions

- The Czech Republic shall create conditions within cyberspace for a smoothly functioning information society.
- The Czech Republic shall aim at a continuous development of cyber security expertise and of capabilities to resist the newest cyber threats. At the same time, it shall support and develop the prevention and early warning capacities of the state security forces.
- The Czech Republic, as a modern Central European country and an active member of the European Union (EU), the North Atlantic Treaty Organisation (NATO), the United Nations (UN) and other international organizations, shall aspire to play a leading role in the cyber security field within its region and in Europe.
- The Czech Republic shall actively support its international partners in preventing and solving cyber attacks, fulfil its commitments arising from the membership in international organizations and from the collective defence within the NATO, and promote security in other states.
- The Czech Republic shall, through its membership in international organizations, actively promote cyber security and defence cooperation and dialogue among Central European countries.
- The Czech Republic shall effectively secure not only individual elements of its critical information infrastructure (hereinafter "CII"), but also ensure the overall security of networks and cyberspace used by its population, which are essential to the latter's economic and social interests.
- The Czech Republic shall particularly focus on securing industrial control systems included in the CII and within a few years shall become one of the leading nations in this area by virtue of the expertise and knowledge acquired.

- The Czech Republic, namely GovCERT.CZ[2], shall seek to build trust and develop an efficient cooperation model with the national CERT[3], while at the same time functioning as an umbrella authority for other Czech CERT/CSIRT teams and promoting creation and development of thereof within CII entities.
- The Czech Republic shall cooperate with private sector and academia in research and development activities concerning security of information and communication technologies.
- The Czech Republic shall strive to ensure maximum cyberspace security. In parallel, it shall support high technologies production, research, development, and implementation, thereby contributing to technological advancement in the Czech Republic with a view to increasing its competitiveness and creating optimal conditions for local and international investments, to which a functional information infrastructure is crucial.
- The Czech Republic shall encourage development of an information society culture through awareness raising among its citizens and private sector subjects. They shall have free access to information society services and to information on responsible behaviour and use of information technologies. The citizens shall be protected from malicious impacts of cyber attacks that could negatively affect quality of their lives and their trust in the state.

[2] GovCERT.CZ is the government coordination unit for rapid reaction to cyber incidents (Government CERT-Computer Emergency Respponse Team) which is subordinated to the National Security Authority, namely the National Cyber Security Centre.
[3] National CERT is the national coordination unit for rapid reaction to cyber incidents (national CSIRT – Computer Security Incident Response Team), which performs its function on the basis of a Memorandum concluded with the National Security Authority.

Principles

Protection of fundamental human rights and freedoms and of the democratic rule of law principles

In ensuring cyber security, the Czech Republic abides by fundamental human rights, democratic principles and values. It respects the Internet's open and neutral character, safeguards the freedom of expression, personal data protection and the privacy rights. It therefore strives for a maximal openness in access to information and for a minimal interference in individuals' and private entities' rights. Protection of the rights pertaining to informational self-determination constitutes one of the basic principles of the National Security Authority's (hereinafter "NSA") activities in the cyber security field.

Comprehensive approach to cyber security based on principles of subsidiarity and cooperation

The Strategy follows the principle of indivisible security; the Czech Republic's cyber security is thus indivisible from global, namely Euro-Atlantic cyber security. The Czech Republic therefore addresses its cyber security in a complex manner as a closely inter-related phenomenon.

The NSA is the primary national authority for cyber security; as such it coordinates cyber security related activities and provides guidance to other entities concerned. The NSA decides on proposals and guidelines for prevention and solution measures in respect of cyber security incidents and ongoing cyber attacks.

Taking into account the complexity of cyber security and defence and with the aim of facilitating the stakeholders' cooperation, promoting synergies of their efforts and avoiding unnecessary duplications, the Czech Republic shall apply the subsidiarity principle and coordinate activities at the national level[4].

[4] The subsidiarity principle also underlies the Act on Cyber Security which sets out responsibilities of a system administrator or operator in respect of system or network security and divides the cyberspace responsibilities between the government and national CERTs.

Trust building and cooperation among public and private sector, and civil society

The state and its agencies cannot bear the sole responsibility for cyber security; an active cooperation of the Czech Republic's citizens, private legal persons and individual entrepreneurs is needed.

Cyberspace and, particularly, a part of the CII are largely owned and operated by the private sector. The security policy for this area is therefore based on inclusive cooperation between the public and the private sectors, civil society, as well as with academia. A trustworthy environment enabling cooperation is crucial. Trust among the state, private subjects, and civil society in general is essential in order to provide cyber security efficiently.

Due to the increasingly blurred lines between internal and external threats and risks, and hence between internal and external security, the Czech Republic shall aim at coordination of activities and enhance mutual trust among stakeholders both at the national and international levels.

Cyber security capacity building

Considering the society's substantial reliance on information and communication technologies and the constantly changing nature of cyber threats and risks, the cyber security of the Czech Republic depends on a continuous development of a robust and resilient information infrastructure, but also on the society as a whole.

The Czech Republic therefore increases its investments in research and development in the cyber security field (including of its own cyber security technologies), as well as in training and education of the end users, i.e. the Czech Republic's population.

In the context of ensuring cyber security, the Czech Republic builds and continuously enhances the national expert capacities and reinforces the existing structures and cooperation procedures relied on to fight cybercrime. Strengthening cooperation between law enforcement bodies and agencies responsible for cyber security in the Czech Republic constitutes thus one of the priorities.

Challenges

1. The Czech Republic as a potential test bed

As a country using advanced security technologies employed also by other countries, the Czech Republic may be targeted as a test bed for a major attack on our allies or states with a greater strategic importance and which use the same technologies, security mechanisms, and procedures.

2. Lack of the public's trust in the state

The public's trust in states as entities ensuring cyber security and in their security structures has significantly decreased recently. Without trust and voluntary participation of the Czech citizens and the private sector, however, the whole concept of cyber security loses its meaning.

3. Increased number of Internet and ICT users and increased criticality of technology failures

The increasing number of Internet users (about 67% of Czech households are online[5]) and ICT users, together with the increasing ICT dependency of the public and private sectors (97% of Czech companies are online[6]) carry an increased criticality of such technologies' potential failure, especially when CII and important information systems (hereinafter "IIS") are involved.

4. Amount of mobile malware increasing along with the number of mobile devices users

Few smartphone and tablet users use at least basic security tools (e.g. antivirus software). This gap is exploited by hackers, as the increasing amount of malware and number of attacks aimed at such devices show every year.

---

[5] Czech Statistical Office, *Information society in figures 2014*, available at www.czso.cz.
Data quoted for year 2013.
[6] EEIP independent study 'Czech Internet Economy' from 2013, available at www.studiespir.cz.

5. **Possible information exfiltration through a hardware backdoor**

The increasing number of technology users and providers carries the risk of 'backdoors' intentionally planted into the hardware. Those may subsequently be misused e.g. for strategic, personal, or sensitive data tracking and mining.

6. **Internet of Things**

While the number of online devices is expanding, most users ignore the necessary digital hygiene, i.e. how to behave online and how to secure the devices they use. The 'Internet of Things' concept amplifies this challenge: while traditional electronic devices such as personal computers and laptops automatically connote antivirus software, firewalls, etc., it is not so with other smart equipment like TV sets, refrigerators etc., users of which often do not even know how to secure its functioning.

7. **Security risks related to IPv4 to IPv6 transition**

The necessary transition from IPv4 to IPv6 protocol brings about new cyber security risks. These risks must be minimized in order to successfully implement and secure this protocol both at the public administration level and in private entities.

8. **Security risks related to the electronisation of public administration (eGovernment)**

The continuing digitalization of public administration in the Czech Republic aims to improve its functioning and its relationship with the public. Nevertheless, services and applications provided to citizens and private entities through eGovernment carry significant cyber risks.

9. **Insufficient security of small and medium enterprises**

There is a growing need to raise awareness of best practices and methods of information infrastructure protection and safe information processing in small and medium enterprises, thereby helping them deal with cyber attacks.

They often fail to acknowledge their own value and their cyber security needs, while simultaneously lacking the resources and know-how necessary to address them. Their systems and data, however, may present the same criticality as those of big enterprises or, alternatively, these small and medium enterprises may work with critical data or systems as sub-contractors.

10. Big data, new data storage environments

Protection and security of data, especially of those of public interest (data relevant to CII and IIS) are crucial for the Czech Republic. The amount of data processed in both public and private sectors is growing and so is the need for their storage. New forms of data storage such as cloud storage have thus appeared. Nevertheless, the use of online services and clouds often leads to non-transparent security solutions of doubtful credibility.

11. Protection of industrial control systems and of information systems in health sector

Cyber attacks have been shifting their focus from direct financial benefit towards industrial cyber espionage, cyber vandalism and identification of CII and IIS vulnerabilities. The attackers focus more and more on information infrastructure elements such as energy supply systems, pipelines or information systems in the health sector. A failure of such systems can have fatal consequences, yet they show high heterogeneity of technical solutions, which also renders any ex post analysis technically difficult.

12. Smart grids

Smart grids constitute a potential next step in the development of the Czech Republic's energy distribution network. These technologies may improve the reliability, security and efficiency of energy networks. On the other hand, digitalisation of these formerly passive systems implies the risk of the network's disruption by an attacker or interference with its users' privacy.

13. Increased ICT dependence of the state's defence forces

Information and communication technologies are increasingly present in the state defence forces' systems, networks as well as equipment proper (for instance, military vehicles or aircraft). Vulnerabilities of these technologies and the danger of their disruption or destruction, including by a cyber attack, increase the risks of a negative impact on basic defence capabilities of the forces and on the fulfilment of commitments arising from the NATO and EU membership. The state defence forces must have the capability to effectively respond to threats coming from cyberspace and to proactively participate in elimination thereof.

14. Increasingly sophisticated malware

The growing sophistication of malware and of attackers themselves significantly limits the options for attack source tracing, i.e. reverse engineering and forensic analysis (backtracking). These analytical procedures shall form part of training of cyber security experts.

15. Botnets and DDoS/DoS attacks

Botnets, used for the very common DDoS/DoS attacks, are gaining on robustness, resilience and stealth. It is therefore necessary to raise awareness of defence possibilities with regard to DDoS/DoS attacks.

16. Increase in cyber crime

Due to the open and anonymous nature of the Internet, possibilities of trade in sensitive information, accessibility and even free purchasing of criminal activities continue to grow. The ongoing expansion of information technologies into the society’s daily life and functioning also results in a swift transition of numerous criminal activities into virtual space which provides the perpetrators with a rapid gain while significantly reducing the risk of prosecution. This phenomenon is enhanced by Internet's anonymity and spatial indefinability. All this allows for precisely targeted as well as mass and large surface attacks.

17. Threats and risks related to use of online social networks

The increasing numbers of social networks users lead to an increased risk of private data theft or even digital identity theft targeting both natural and legal persons.

18. Low digital literacy of end users

A substantial number of Internet users – both in the public sector and the general public – lack a basic knowledge on common computer attack methods (especially phishing, fake e-shops etc.), which leads to thousands of the Czech Republic's citizens becoming victims of such attacks every year.

19. Shortage of cyber security experts and the need for curricula reform

The existing Czech education model in the cyber security field does not meet current needs and trends. It does not provide adequate knowledge to primary and secondary level students, or enough university programs that would produce cyber security experts. Yet, the demand for such experts is high.

Main goals

A. Efficiency and enhancement of all relevant structures, processes, and of cooperation in ensuring cyber security

- To develop an effective cooperation model at the national level among the cyber security actors – CERT and CSIRT teams, CII subjects, etc. and reinforce their existing structures and processes.
- To develop a national incident handling procedure that will set a cooperation format, contain a communication matrix, a procedure protocol and define each actor's role.
- To develop a risk assessment methodology at the state level.
- To 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.[7]
- To 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).

[7] The specific procedure for coordination with other agencies involved shall be treated in the Action Plan.

B. Active international cooperation

- To engage actively in international discussion taking place in the fora, programes and initiatives of the EU, the NATO, the UN, the Organization for the Security and Cooperation in Europe, the International Telecommunication Union and other international organizations.
- To promote cyber security and inter-state dialogue within the Central European region.
- To establish and deepen bilateral cooperation with other states.
- To participate in and organize international exercises.
- To participate in and organize international trainings.
- To participate in creation of an efficient cooperation model and in confidence building among CERT and CSIRT teams at international level, international organizations and academia.
- To contribute to fostering an international consensus, within formal and informal structures, on legal regulations and behaviour in cyberspace, safeguarding of an open Internet, and human rights and freedoms.

C. Protection of national CII and IIS

- To pursue a continuous analysis and control of CII and IIS security in the Czech Republic based on a clearly defined protocol.
- To support creation of new CERT and CSIRT teams in the Czech Republic.
- To enhance, on a continuous basis, the CII and IIS networks' resistance, integrity and trustworthiness.
- To analyse and monitor, on a continuous basis, the threats and risks in the Czech Republic.
- To share, in an efficient manner, information among the state and CII and IIS subjects.
- To 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.

- To secure in a thorough and reliable manner a CII and IIS data storage environment to be established and managed by the state.
- To 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.
- To enhance, on a continuous basis, technological and organizational prerequisites for active countering (suppression) of cyber attacks.
- To increase national capacities for active cyber defence and cyber attack counter-measures.
- To train experts specialised in questions of active counter-measures in cyber security and cyber defence and in offensive approach to cyber security in general.
- To 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.

D. Cooperation with private sector

- To continue cooperation with private sector and raise general awareness of the NSA's activities in the cyber security field.
- To create, in cooperation with private sector, uniform security norms, standardize the cooperation and set an obligatory protection level for CII subjects.
- To 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.
- To 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.
- To 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.

E. Research and development / Consumer trust

- To participate in national and European research projects and activities concerning cyber security.
- To 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.
- To 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.
- To 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.
- To make research and development a national priority and thereby actively stimulate investments in this field.

F. Education, awareness raising and information society development

- To 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.
- To modernize the existing primary and secondary school curricula and support new university study programs designed to produce cyber security experts.
- To provide relevant education and training to public administration staff involved, but not exclusively, in the field of cyber security and cybercrime.

G. Support to the Czech Police capabilities for cybercrime investigation and prosecution

- To reinforce the personnel of individual cybercrime police departments.
- To modernize technological equipment of specialized police departments.
- To establish direct and prompt cooperation links for the field of cybercrime between relevant national entities and other security forces.
- To support international cooperation in information sharing and training in the field of cybercrime.
- To provide professional education and training to police specialists.
- To create a multidisciplinary academic environment to enhance the Czech Police capacities in cybercrime prosecution.

H. Cyber security legislation (development of legislative framework). Participation in creation and implementation of European and international regulations.

- To create a comprehensible, effective, and adequate cyber security legislation based on systemic approach and taking into account the existing legislation.
- To participate actively in creation and implementation of European and international regulations.
- To 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.
- To support cyber security related education of the judiciary (ie. Prosecutors or judges).

Implementation

Based on the main goals of the Strategy and in coordination with all stakeholders involved, an **Action Plan** is prepared to define specific steps, responsibilities and deadlines for their fulfilment and auditing[8].

The NSA and the NCSC as its specialized department shall continuously monitor, discuss, and evaluate, in cooperation with other stakeholders, the levels of achievement of individual goals. It shall submit an annual "Report on the State of Cyber Security in the Czech Republic" to which information on fulfilment of the Action Plan shall be annexed. The report shall inform the government and the general public on effectiveness of measures adopted and on progress in fulfilment of tasks defined by the Strategy.

[8] The Action Plan is expected to be adopted by the Government of the Czech Republic during the second quarter of 2015.

Annexes

Annex No. 1

List of abbreviations

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

DDoS/DoS – Distributed Denial of Service / Denial of Service

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

CII – Critical Information Infrastructure

IIS – Important Information System

NSA – National Security Authority

NCSC – National Cyber Security Centre

Annex No. 2

Glossary[9]

Botnet

Network of infected computers controlled remotely by a bot master which can thus access thousands of machines at the same time. It allows illegal activities on a large scale – in particular, attacks such as DDoS and spam distribution.

Cloud / Cloud storage

Digital data storage model for online environment.

DDoS / DoS attacks

Attack techniques from many vectors on the internet services or pages, resulting in requests flooding or breakdown or non-functionality or unavailability of the system for other users.

Forensic analysis

Investigative approach to digital data, which aims to obtain evidence on user's (attacker) activities.

Hacktivism

Hacking services use for social or political goals.

Malware

General term for malicious programs including computer viruses, Trojan horses, worms, spyware.

Reverse engineering

Reverse analysis of the malware in order to extract the design and functioning principles.

Penetration testing

Analysis of functions of a computer system and networks, with the objective of finding out weak spots in computer security so that these could be removed.

[9] A more ample thesaurus for cyber security is available on the www.govcert.cz site.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu