DOI 10.15302/J-SSCAE-2016.06.008

Research on a Cybersecurity Review System with Suggestions

Chen Xiaohua[1]**, He Dequan**[2]**, Wang Hailong**[3]**, Shang Yanmin**[4]**, Xu Kefu**[4]

1. Chinese Academy of Cyberspace Studies, Beijing 100010, China
2. China Information Technology Security Evaluation Center, Beijing 100085, China
3. Institute of Computer Technology, Chinese Academy of Sciences, Beijing 100190, China
4. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract: Cybersecurity is a part of national security. The rules and regulations for security testing and evaluation are established in policies regarding national security review systems or cyberspace management. This paper focuses on current international systems related to cybersecurity reviews, and analyzes foreign governments' practices in information technology (IT) product and service security evaluations, critical information infrastructure (CII) security evaluation and management, information and communication technology (ICT) supply chain security and background security investigation. Based on this information and analysis, the authors research how to establish a China's cybersecurity review system in the areas of law and regulation, organization framework, operation mode, review approach, and supporting technology.

Keywords: cybersecurity review; information technology products and services; critical information infrastructure; ICT supply chain security; background security

1 Introduction

Because cyberspace is currently the main area of competition for countries around the world, security risks including technology vulnerabilities and product "backdoors" may bring heavy losses to any country. The documents disclosed by Edward Snowden, a former employee of the National Security Agency, revealed that the US intelligence agencies had many famous American information technology (IT) firms involved in the PRISM program, which aimed to steal cyber information and spy on governments and "netizens" (Internet users) around the globe. At present, chips, operating systems, databases, and critical technologies in the China's market are still overshadowed by those from other countries, resulting in serious security threats. At the same time, the products of China's information and communication technology (ICT) enterprises are facing rigorous reviews in foreign countries, and their commercial activities, such as acquisitions in the international market, have repeatedly been interfered with and blocked.

This paper focuses on researching foreign systems related to cybersecurity reviews, and provides a reference for the establishment of a China's cybersecurity review system.

2 Overview of foreign systems related to cybersecurity reviews

Western countries such as the US and UK have relatively mature national security review systems, and have successfully established security investigation and evaluation systems for ICT products, services, and providers. To date, no report exists on the establishment of a special cybersecurity review system in a foreign country. However, according to the national security reviews and information security management systems, foreign countries have carried out rigorous work related to cybersecurity reviews.

Received date: 12 October 2016; **revised date:** 17 October 2016

Corresponding author: Chen Xiaohua, Chinese Academy of Cyberspace Studies, Vice President and Researcher. Major research fields include cybersecurity review, network security evaluation and standard, cloud computing, and big data security. E-mail: chenxhcn@263.net

Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)

Chinese version: Strategic Study of CAE 2016, 18 (6): 039–043

Cited item: Chen Xiaohua et al. Research on a Cybersecurity Review System with Suggestions. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.008

2.1 US laws and policies related to cybersecurity reviews

As one of the first countries to conduct a national security review, the US has relatively complete rules and regulations; these include the Federal Acquisition Regulation (FAR) [1], the Foreign Investment and National Security Act of 2007 (FINSA 2007) [2], and the Exon-Florio Provision [3].

The US takes advantage of its economic and technical edge in its information security industry and in professional testing organizations in order to follow trends in national standardization strategies and policies, thus ensuring its leadership in setting international standards. Any foreign enterprise hoping to operate in the US cyberspace must pass a national security review and sign a security agreement with US security departments. This agreement covers stipulations regarding the privacy rights of citizens, data and file storage reliability, and ensuring effective monitoring enforced by US network law enforcement departments.

2.2 The federal information security management act

The Federal Information Security Management Act (FISMA) [4] involves a series of standards, guides, and report requirements to ensure the security management of government information systems.

FISMA regulated corresponding responsibilities to ensure the information system security of federal organizations, the National Institute of Standards and Technology (NIST) [5], and the Office of Management and Budget (OMB) [6]. It required every federal organization to develop and perform relevant documents to ensure information security and information system security, thus supporting the operation of these organizations and protecting federal assets.

2.3 US national security review organization

The Committee on Foreign Investment in the United States (CFIUS) [7] is a trans-department organization that consists of representatives of the US Department of Defense, the US Department of State, the US Department of Homeland Security, and so forth. The CFIUS president is also Secretary of the US Department of the Treasury. In addition, the person in charge of coordinating CFIUS is the Director of the US Department of the Treasury Office of Investment Security, and is responsible for accepting, handling, and coordinating merger and acquisition (M&A) applications. CFIUS reviews any transactions of foreigners that may control American enterprises in order to determine the influence of these transactions on the US national security; however, the execution details are not completely clear and transparent.

The US House of Representatives Permanent Select Committee on Intelligence once carried out an investigation on the China's telecom operators Huawei and ZTE regarding national security reviews [8]. This investigation was conducted in various ways, and included holding interviews with enterprise staff, checking document materials, holding hearings, and conducting a field investigation. It is worth mentioning that these companies' relationships with the government, the political parties, the military, and the intelligence departments were the main focus of the investigation. The committee finally proved the possibility of these companies posing a threat to national security, based on materials on the words, actions, and background of senior executives and core staff of these enterprises, and on information on the internal and external operation, intellectual property, and R&D of the enterprises.

2.4 IT products and services security evaluation in the US and the UK

2.4.1 IT security certification in the US

The US requires any information security products entering the national security system and commercial off-the-shelf (COTS), as well as information assurance (IA)-enabled products, to pass the evaluation and certification of the National Information Assurance Partnership (NIAP) [9] Common Criteria Evaluation and Validation Scheme (CCEVS). Any government department purchasing products of this kind must select products that meet security requirements from lists of products passing the NIAP certification [10]. Note that the phrase "national security system" refers to information systems in US government departments that handle sensitive information, including confidential information and information related to military affairs and intelligence.

2.4.2 UK information product technology check

The Communications Electronics Security Group (CESG) [11] is responsible for overall information product security certification in the UK. A source code check is an important mean of implementing certification, and commercial organizations recognized by CESG are commissioned to conduct specific certification and testing.

2.4.3 US cloud computing service security evaluation

The Federal Risk and Authorization Management Program (FedRAMP) [12] presents standard methods for security evaluation, authorized use, and continuous monitoring of the cloud service in the US. Federal agencies can use FedRAMP's authorized cloud service to deploy their information system, thus ensuring repeated use with a one-time authorization.

2.5 Critical information infrastructure security management and evaluation

As critical information infrastructure (CII) security is a key part of cybersecurity in the US, national critical information infrastructure protection (CIIP) can be treated as a risk-management process. Any damage or failure caused to any system or asset of this sort can have negative impacts on a country's national security, economic security, public health and security, or any set of items mentioned above.

In the US, the Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center (NIPC) are responsible for early CIIP policy coordination. The Homeland Security Act of 2002 regulated the establishment of the Department of Homeland Security [13] to replace CIAO and NIPC. At the same time, it also established other special organizations, including the Department of Agriculture, Department of Health and Human Services, Environmental Protection Agency, Department of Energy, Department of the Treasury, and Department of Defense. The US adopted various measures [14,15] (including the development of a national strategy, presidential proclamation, executive order, and law) to enhance the protection for critical infrastructure (CI) and CII.

2.6 Supply chain security management

The US always focuses on supply chain security, and has introduced a series of policies and documents on this topic. These include the Strategy to Enhance International Supply Chain Security [16], the Federal Plan for Cyber security and Information Assurance Research and Development [17], the Comprehensive National Cybersecurity Initiative [18], and the Cyberspace Policy Review. These policies and documents show that the US has lifted IT supply chain security to the same level as security regarding national threats and confrontation. The NIST is responsible for developing standards, guides, and testing and measuring indexes for the protection of non-national security federal information and communication infrastructure. It has also researched and developed ICT supply chain risk management (SCRM) tools and indexes, and guides on mitigation measures and implementation methods [19–23].

2.7 Staff background investigation

A staff background investigation, also known as a loyalty investigation in the US, is a systematic job involving various departments, processes, and factors and including a huge amount of deskwork and field visits.

The Office of Personnel Management (OPM) [24] is a US government agency responsible for setting the overall principles and general management rules for a background investigation. Background investigations should be initiated for any areas that involve national security or that are confidential [25,26]. For national security, OPM currently classifies the positions of all federal agencies and the majority of government contractors into six categories, with 10 corresponding management standards and requirements, based on sensitivity and risk. OPM set and released Standard Form 86—Questionnaire for National Security Positions [27], which requires a background investigation to be carried out on government employees that may come in contact with classified information. In addition, OPM set and released Standard Form 85—Questionnaire for Non-Sensitive Positions [28], which requires a background investigation to be carried out on government employees or on contracted employees of the government.

3 Thoughts and suggestions on the establishment of a cybersecurity review system in China

3.1 The concept, purpose, and roles of cybersecurity reviews

The basic concept of a cybersecurity review is to conduct evaluation, surveillance, and analysis, and to maintain continuous supervision over the security, controllability, and credibility of the IT products and services used in information systems related to national security and social stability, and of the providers of these products and services.

The direct purpose of a cybersecurity review is to prevent the providers of products and services from being inappropriately controlling, disturbing or destroying user systems, illegally monitoring users in order to gain and use sensitive user information, or illegally collecting, storing, and processing user information.

The key roles of a cybersecurity review are to safeguard the interests of national security; to ensure the security, controllability, and credibility of critical products and services that influence critical information systems and CI; and to enhance the security management of IT products and services.

3.2 Laws and standards

Laws and standards can ensure the legitimacy, coerciveness, and enforceability of cybersecurity reviews. In China, the legal basis of a cybersecurity review mainly stems from the following items:

- The National Security Law of the People's Republic of China and the Cybersecurity Law of the People's Republic of China;
- Rules and regulations on government information system management and purchases, IT products and services, CII, and ICT supply chain security management;
- Cybersecurity review management measures and enforcement regulations; and
- International norms such as those established by the World Trade Organization (WTO).

In addition, technical and management standards should be set for software security reviews, equipment security reviews, service security reviews, development process security reviews, and background reviews.

3.3 Organization system

A practical organization system is the key to conducting a cybersecurity review. The main organizations and functions of the organization system are as follows:

- The trans-department cybersecurity review committee is responsible for the overall arrangement of cybersecurity reviews and coordination; it consists of representatives from relevant departments;
- The expert advisory committee is responsible for offering advice regarding cybersecurity reviews;
- The management office is an administration organization for cybersecurity reviews, and it is responsible for organization and implementation;
- The implementing agency carries out the review; and
- The technology supporting agency provides technologies.

3.4 Operation mode

3.4.1 Review objects

The objects of a cybersecurity review are IT products and services and the providers of these products and services. The objects to be reviewed include:

- Products, services, and providers related to CII;
- Products, services, and providers related to the critical information systems of state and government departments;
- Products, services, and providers that are endangering the political structure, the community, or the economy;
- Products, services, and providers that are doing harm to public interests; and
- Products, services, and providers that are commonly used, have a huge influence, and pose a threat to national security.

3.4.2 Review content

The content of a cybersecurity review covers the security, controllability, and credibility of IT products and services and the providers of these products and services.

Security includes physical security, logical security, and security management. Physical security involves providing physical protection to relevant system devices and facilities to prevent them from being damaged or lost; logical security refers to the security of information resources in relevant systems, and includes confidentiality, integrity, and availability; and security management involves various security management policies and mechanisms.

Controllability requires security monitoring to be conducted on products and services to ensure that IT products and services provide due services that are based only on users' commands, thus achieving the goal of monitoring and managing IT risks and auditing processes, such as traceability, confirmability, auditability, and reviewability.

Credibility requires enterprises (including supply chains) and the core staff of the enterprise to demonstrate relevant skills, meet management requirements, provide clarification materials, answer set questions, and have the ability to bear an investigation review, all within a required time and scope. In this way, enterprises can reach a trusted level in the security and controllability of IT products and services and in national security, as well as meeting preset and acceptable trust standards as verified by the information and evidence collected by the review team.

3.4.3 Initiation condition

The initiation of a cybersecurity review process should meet one of the following conditions:

- It should be according to the clear stipulations of laws and regulations;
- It should be a response to complaints or to the report of an offence;
- It should be based on a market study or the results of spot checking;
- It should be applied voluntarily; or
- It should meet other necessary conditions.

3.4.4 Review approach

Background reviews carried out on IT products and services are intended to improve a country's control over the credibility of IT products and services. The core work involved in a background review is information collecting, mining, analyzing, and searching.

(1) Enterprise background review

A background review of an enterprise focuses on the following aspects:

- The enterprise's relationship with the government, political parties, military, and intelligence departments;
- Its reputation;
- Its qualifications;
- Its operation condition;
- Its credit record;
- Its criminal record;
- Its production environment;
- The management and implementation departments of the enterprise; and
- Its staff allocation and other aspects.

(2) Supply chain review

An enterprise's background review must include a review of its supply chain; this mainly considers the management system and the implementation of suppliers. The main focuses of a supply chain review include technology, quality, response, delivery, cost, environment, social responsibility, and cybersecurity.

(3) Staff background review

Staff includes senior executives (such as founders, board members, and chief officers), chief product designers, and chief product developers, whether or not these people are still with the enterprise. The main content of a staff background review includes the following factors:

- Political experience;
- Work experience;
- Criminal record;
- Credit record;
- Physical condition;
- Household condition;
- Mental status; and
- Any antihuman statements or actions that the staff member has made or performed, and so forth.

(4) Questionnaires

Questionnaires are an important basis of a background investigation. They show the initial assessments on the objects of the investigation and require several interactions with the objects of the investigation. The following guidelines should be followed during the use and design of a cybersecurity review questionnaire.

- Use the questionnaire cautiously;
- Ensure that the topic of the questionnaire is systematically covered, targeted, general, and different from other topics;
- Combine multiple choice questions with essay questions; and
- Incorporate reasonable evaluation principles.

3.4.5 Supporting technology

(1) Facing a background review

All the intelligence collected during a background review (including the supply chain) should be fully processed, analyzed, and evaluated in order to discover any hidden threats in national security. Intelligence processing mainly comprises intelligence collection, follow-up investigations, evidence mining, intelligence associations, big data analysis, knowledge base or database, risk assessment, demand assessment, judgment and decision making, and other supporting technologies. Even though some of these technologies are now mature, their application in background reviews still requires further improvement and optimization in order to meet necessary demands.

Big data analysis is the core supporting technology of a background review, because a background review requires continuous follow-up investigations regarding the overall situations of domestic and foreign IT enterprises. It also requires storing, sorting out, checking, updating, and maintaining all evidence information, and thus providing historical materials and data support for the next review.

(2) Facing a technology review

A security risk analysis is the main means of supporting a technology review, and includes a source code review, reverse engineering, and penetration testing.

4 Conclusions

At present, Russia, Japan, Australia, India, and other countries are establishing and perfecting their systems related to cybersecurity reviews; these countries mainly focus on information industry security reviews of foreign M&A, information products' market access, and information products' security certification.

Using the experience of other countries as a reference, the establishment of a China's cybersecurity review system should focus on the following aspects: ① strengthening publicity and improving the public's understanding of what a cybersecurity review is; ② constituting measures regarding policy support, mechanism building, team construction, talent cultivation, and so on; and ③ paying attention to background reviews and technique and developing a supporting information system for a cybersecurity review.

References

[1] General Services Administration (GSA), U.S. Department of Defense (DoD), National Aeronautics and Space Administration (NASA). Federal acquisition regulation (FAR), FAC 2005_91 [Z/OL]. (2016-09-29) [2016-10-12]. https://www.acquisition.gov/?q=browsefar.

[2] U.S. Congress. Public law 110–49：Foreign investment and national security act of 2007 (FINSA) [Z/OL]. Washington, DC: U.S. Government Printing Office, (2007-07-26) [2016-10-12]. https://www.gpo.gov/fdsys/pkg/STATUTE-121/pdf/STATUTE-121-Pg246.pdf.

[3] Peterson Institute for International Economics. The Exon-Florio Amendment [Z/OL]. Washington, DC: Peterson Institute for International Economics. (2016-04-25) [2016-10-12]. https://piie.com/publications/chapters_preview/3918/02iie3918.pdf.

[4] U.S. Department of Homeland Security. Federal information security management act (FISMA) [Z/OL]. (2016-10-03) [2016-10-12]. https://www.dhs.gov/fisma.

[5] National Institute of Standards and Technology (NIST) [EB/OL]. [2016-10-12]. http://www.nist.gov/.

[6] Office of Management and Budget (OMB) [EB/OL]. [2016-10-12]. https://www.whitehouse.gov/omb.

[7] The committee on foreign investment in the United States (CFIUS) [EB/OL]. [2016-10-12]. https://www.treasury.gov/resource-center/international/Pages/Committee-on-Foreign-Investment-in-US.aspx.

[8] Rogers M, Ruppersberger D. Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE [J]. Journal of Current Issues in Media & Telecommunications, 2012, 4 (2): 59.

[9] National Information Assurance Partnership (NIAP) [EB/OL]. [2016-10-12]. https://www.niap-ccevs.org/.

[10] NIAP. CCEVS objectives [EB/OL]. [2016-10-12]. https://www.niap-ccevs.org/Big_Picture/objectives.cfm.

[11] Communications-Electronics Security Group (CESG) [EB/OL]. (2012-05-14) [2016-10-12]. http://whatis.techtarget.com/definition/CESG.

[12] Federal Risk and Authorization Management Program (FedRAMP) [EB/OL]. (2016-10-05) [2016-10-12]. https://www.fedramp.gov/about-us/about/.

[13] U.S. Department of Homeland Security (DHS) [EB/OL]. [2016-10-12]. https://www.dhs.gov/.

[14] U.S. Department of Homeland Security. Homeland security presidential directive 7: critical infrastructure identification, prioritization, and protection [EB/OL]. (2015-09-22) [2016-10-12]. https://www.dhs.gov/homeland-security-presidential-directive-7.

[15] The White House. Executive order—improving critical infrastructure cybersecurity [EB/OL]. (2013-02-12) [2016-10-12]. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[16] U.S. Department of Homeland Security. Strategy to enhance international supply chain security (July 2007) [EB/OL]. (2015-07-14) [2016-10-12]. https://www.dhs.gov/publication/international-supply-chain-security.

[17] Cyber Security and Information Assurance Interagency Working Group (CSIA IWG). Federal plan for cyber security and information assurance research and development [R]. Washington, DC: CSIA IWG, 2006.

[18] The White House. The comprehensive national cybersecurity initiative [EB/OL]. [2016-10-12]. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[19] National Institute of Standard Technology. Standards for security categorization of federal information and information systems, FIPS PUB 199 [S]. Gaithersburg: NIST, 2004.

[20] National Institute of Standard Technology. Minimum security requirements for federal information and information systems, FIPS PUB 200 [S]. Gaithersburg: NIST, 2006.

[21] National Institute of Standard Technology. Summary of NIST SP 800-53 revision 4, security and privacy controls for federal information systems and organizations [S]. Gaithersburg: NIST, 2014.

[22] National Institute of Standard Technology. Guideline for identifying an information system as a national security system, SP 800-59 [S]. Gaithersburg: NIST, 2003.

[23] National Institute of Standard Technology. Guide for mapping types of information and information systems to security categories, SP 800-60 [S]. Gaithersburg: NIST, 2008.

[24] U.S. Office of Personnel Management (OPM) [EB/OL]. [2016-10-12]. https://www.opm.gov/.

[25] Farrell B S. Personal Security Clearances: Actions needed to ensure quality of background investigations and resulting decisions [R]. Washington, DC: U.S. Government Accountability Office, 2014.

[26] Federal Investigative Services. The security clearance and investigation process [R/OL]. Washington, DC: U.S. OPM. [2016-10-12]. http://www.brac.maryland.gov/documents/security%20clearance%20101%20pp%20presentation.pdf.

[27] U.S. Office of Personnel Management. Questionnaire for national security positions, OMB No. 3206 0005 [Z/OL]. Washington, DC: U.S. OPM, 2010 [2016-10-12]. https://www.opm.gov/forms/pdf_fill/sf86.pdf.

[28] U.S. Office of Personnel Management. Questionnaire for non-sensitive positions, OMB No. 3206-0261 [Z/OL]. Washington, DC: U.S. OPM, 2013 [2016-10-12]. https://www.opm.gov/forms/pdf_fill/sf85.pdf.