CYBERWELLNESS PROFILE UNITED STATES

BACKGROUND

Total Population: 315 791 00
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 84.20%
(data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- 15 USC Chapter 103 - Controlling the Assault of Non-solicited Pornography and Marketing
- 18 USC, Chapter 47, § 1029 - Fraud and related activity in connection with access devices
- 18 USC, Chapter 47, § 1030 - Fraud and related activity in connection with computers
- 18 USC, Chapter 47, § 1037 - Fraud and related activity in connection with electronic mail
- 18 USC Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 USC Chapter 121 - Stored Wire and Electronic Communications and Transactional Record Access

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- 44 USC Chapter 35, Subchapter III
- Uniform Electronic Transactions Act
- Homeland Security Act
- Protecting Children in the 21st Century Act
- Adam Walsh Child Protection and Safety Act
- Freedom of Information Act (5 USC § 552)
- Information Security (§3541)
- Electronic Signatures in Global and National Commerce Act
- Cyber Security Research and Development Act
- Children's Internet Protection Act
- Keeping the Internet Devoid of Sexual Predators Act
- Privacy Act (5 U.S.C. § 552a)
- Federal Information Security Management Act of 2002

1.2 TECHNICAL MEASURES

1.2.1 CIRT

United States has an officially recognized national CIRT (US CERT) and an industrial control systems CERT (ICS-CERT).

1.2.2 STANDARDS

United States has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:

- National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.0
- Federal Information Security Management Act of 2002
- NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems"
- The North American Electric Reliability Corporation (NERC) has created many standards. The most widely recognized is NERC 1300 which is a modification/update of NERC 1200.
- National Institute of Standards and Technology Special publication 800-12 provides a broad overview of computer security and control areas.

1.2.3 CERTIFICATION

The National Initiative for Cybersecurity Education (NICCS) offers a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

United States has officially recognized International Strategy for Cyberspace. There is also an executive order in order to improve critical infrastructure cybersecurity. A Critical Infrastructure Protection Program has been in place since 1996.

1.3.2 ROADMAP FOR GOVERNANCE

The NIST Roadmap for Improving Critical Infrastructure Cybersecurity, the Cross-Sector Roadmap for Cybersecurity of Control Systems and the Roadmap to achieve energy delivery systems cybersecurity provide the national governance roadmap for cybersecurity in the United States.

1.3.3 RESPONSIBLE AGENCY

The White House has an appointed US Cybersecurity Coordinator at the level of Special Assistant to the President to guide Executive branch efforts. The Department of Homeland Security (DHS) and the Department of Defense (DoD) are the primary cybersecurity actors in order to monitor and coordinate the implementation of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provides detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Department of Defense (DOD) established the Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Program that aims to provide cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. The National Institute of Standards and Technology (NIST) leads also in developing a Cybersecurity Framework of standards and best practices for protecting critical infrastructures.

The Cybersecurity Division (CSD) provides information resources—standards, frameworks, tools, and technologies to enable seamless and secure interactions among homeland security stakeholders and leads the government's charge in funding cybersecurity research and development (R&D).

Also the IT Security Essential Body of Knowledge (EBK) establishes a national baseline of the essential knowledge and skills that IT security practitioners in the public and private sector should have to perform specific roles and responsibilities.

1.4.2 MANPOWER DEVELOPMENT

United States has the following various types of awareness programs, industry talk, conferences, training programs and workshops on cybersecurity, for the general public as well as for public and private sector employees:

- National Cybersecurity Awareness Month
- Stop.Think.Connect. Campaign
- Cyber-Physical Systems Public Working Group Workshop
- National Initiative for Cybersecurity Education
- National Cybersecurity Education Council (NCEC)
- Cybersecurity Education and Training Assistance Program (CETAP)
- National Cybersecurity Workforce Framework - NICCS
- National Centers of Academic Excellence (CAEs) that provide students valuable technical skills in various disciplines of Information Assurance

- The Federal Cybersecurity Training Events (FedCTE) that delivers training, labs, and competitions for Federal cybersecurity and IT professionals.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information regarding any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, United States has officially recognized partnerships with the following organizations:

- DHS and Canada Public Safety Plan to Strengthen Cybersecurity Cooperation
- FIRST
- US CERT
- United States and Estonia: Partners in Cyber Security and Internet Freedom

1.5.2 INTRA-AGENCY COOPERATION

United States has officially recognized the following national or sector-specific programs for sharing cybersecurity assets within the public sector through the Department of Homeland Security (DHS) created by the Homeland Security Act of 2002.

- The National Infrastructure Protection Plan (NIPP)
- The Department of Homeland Security and the Department of Defense (DOD) signed a landmark memorandum of agreement in 2010 to protect against threats to critical civilian and military computer systems and networks.
- The Department of Homeland Security, the Department of Defense, and the Financial Services Information Sharing and Analysis Center launched a pilot initiative designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information.
- The Cybersecurity Partners Local Access Plan.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Administration provides officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through a Cybersecurity Framework, a guide developed collaboratively with the private sector for private industry to enhance their cybersecurity, in 2014.

The National Cybersecurity Center of Excellence (NCCoE) provides businesses with real-world cybersecurity solutions—based on commercially available technologies. Finally the Department of Homeland Security's Critical Infrastructure Cyber Community C^3 Voluntary Program helps align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks.

1.5.4 INTERNATIONAL COOPERATION

United States is signatory to Council of Europe Convention on Cybercrime and there is an EU-US cooperation on cybersecurity and cyberspace.

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child online protection has been enacted through the following instruments:

- Section 15 of the US Code, Chapter 91, §§ 6501-6506, included in the US Code by the Children's Online Privacy Protection Act, 1998.
- Section 47 of the US Code, Chapter 5, §§ 254(h)(6).
- Section 18 of the US Code, Chapter 110, §§ 2251-2260A, amended by H.R. 1981, May 2011.
- Section 20 of the US Code, Chapter 72, §§ 9134 (f), included in the US Code by the Children's Internet Protection Act, 2000.
- Adam Walsh Child Protection and Safety Act, July 2006.
- Securing Adolescents from Exploitation Online Act, February 2007.
- Protect our Children Act, October 2008.
- Keeping the Internet Devoid of Sexual Predators, October 2008.

The International Strategy for Cyberspace does not outline child online protection.

2.2 UN CONVENTION AND PROTOCOL

United States has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

United States has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The following supports provide information on internet safety for parents, children and educators:

- Branch created within the Department of Justice: Internet Crime against Children Task Force.
- The Federal Trade Commission runs the OnGuardOnline website, the federal government website dedicated to bringing information on internet safety.
- Branch created within the US Department of Health and Public Service: Administration for Children and Families.
- Organization authorized to work in partnership with the US Department of Justice: National Center for Missing and Exploited Children.
- The United State Computer Emergency Response Team (US-CERT) does not provide specific information on child online protection but hosts a series of links redirecting to it.

2.4 REPORTING MECHANISM

Complaints can be filed through the OnGuardOnline website. Cyber Tipline of the National Centre for Missing and Exploited Children has a dedicated space to report incidents which include computer incidents related to child online protection.

DISCLAIMER: Please refer to http://www.itu.int/en/Pages/copyright.aspx
More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 14th January 2015