Cybersecurity and Privacy Landscape in United States

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission´s behalf may be held responsible for the use which may be made of the information contained therein.

The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.

TABLE OF CONTENTS

Page

LIST OF ABBREVIATIONS

CAN-SPAM Act: Controlling the Assault of Non-Solicited Pornography and Marketing Act
CERT: Computer Emergency Response Team
CICI: Cybersecurity Innovation for Cyberinfrastructure
CISE: Computer and Information Science and Engineering
CLOUD Act: Clarifying Lawful Overseas Use of Data Act
CONSENT Act: Customer Online Notification for Stopping Edge-provider Network Transgressions Act
COPPA: Children´s Online Privacy Protection Act
cPPP: Contractual Public-Private-Platform on Cybersecurity
CPS: Cyber-Physical Systems
CSIRT: Computer Security Incident Response Team
CSA: Coordination and Support Action
CSDP: Common Security and Defense Policy
DESI: Digital Economy and Society Index
DHS: Department of Homeland Security
DSP: Digital Service Provider
e-Privacy: (Proposed) e-Privacy Regulation
EC3: European Cybercrime Center
ECPA: Electronic Communications Privacy Act
ENISA: European Agency for Network and Information Security
EO: Executive Order
FISMA: Federal Information Security Modernization Act
FITARA: Federal Information Technology Acquisition Reform Act
FTC: Federal Trade Commission
GDPR: General Data Protection Regulation
GLB: Gramm-Leach-Bliley Act or The Financial Services Modernization Act
ICE-T: US-EU Internet Core & Edge Technologies
IoT: Internet of Things
JRC: Joint Research Centre
MLA: Mutual Legal Assistance
MLAT: Mutual Legal Assistance Treaty
NCCIC: National Cybersecurity and Communications Integration Center
NGI: Next Generation Internet
NIST: National Institute of Standards and Technology
NPRS: National Privacy Research Strategy
NSF: National Science Foundation
NSTC: National Science and Technology Council
PCAST: President's Council of Advisors on Science and Technology
R&I/R&D: Research and Innovation / research & Development
RDSP: Federal Cybersecurity Research and Development Strategic Plan
SaTC: Secure and Trustworthy Cyberspace
WG: Working Groups

1 INTRODUCTION

This report on Cybersecurity and Privacy Landscape in the United States, Deliverable 2.2, presents a comprehensive snapshot of the current landscape of the cybersecurity and privacy activities in the United States.

The editorial team took an approach to first define the common terminology and analysis framework that will include technological, policy, economic, legal and regulatory aspects. In so doing, it will consider the specificities of both sides and current as well as proposed legislation.

This approach has resulted in the Cybersecurity and Privacy Landscape in the United States deliverable being divided into four independent sections (not including introduction and conclusions).

Section 2 contains a comprehensive analysis of the cybersecurity and privacy research and innovation topics, taking the critical areas as defined by the Federal Cybersecurity Research and Development Strategic Plan (RDSP[1]) [1], which has identified six areas critical to successful cybersecurity R&D: (1) Scientific Foundations; (2) Risk Management; (3) Human Aspects; (4) Transitioning successful research into practice; (5) Workforce Development; and (6) Enhancing the research infrastructure. Since we couldn't find any specific topics or ongoing projects related to critical area (4), we only analysed this to a certain degree in section 5 of the report. In addition, a sub-section on Frameworks is included in Chapter 2 to capture the substantial activity underway in the US on Frameworks for cybersecurity related subjects.

Section 3 contains an overview of the US Cybersecurity and Privacy strategy to the present day;

Section 4 contains an overview of the US Policies and Legislation activities to the present day;

Finally, **Section 5** presents an analysis of the ongoing activities related to the strengthening of the Cybersecurity and Privacy market in the United States.

[1] Federal Cybersecurity Research and Development Strategic Plan https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

2 CYBERSECURITY AND PRIVACY TECHNOLOGICAL ASPECTS (INCLUDING NEW AND EMERGING TRENDS IN TECHNOLOGIES AS WELL AS THOSE FOR CYBER MENACES)

In terms of Research and Development (R&D) activities in topics related to cybersecurity and privacy in the United States, research was focussed especially within the programmes of the National Science Foundation (NSF); in particular, the most relevant programme funding activities in cybersecurity and privacy is the Secure and Trustworthy Cyberspace (SaTC) program.

In order to structure the topics across thematic areas, the WP2 team decided to structure the topics according to the critical areas as identified by the United States' Federal Cybersecurity Research and Development Strategic Plan (RDSP[2]) [1], which has identified six areas critical to successful cybersecurity R&D:

(1) Scientific Foundations: Cybersecurity needs sound mathematical and scientific foundations with clear objectives, comprehensive theories (e.g., of defense, systems, and adversaries), principled design methodologies, models of complex and dynamic systems at multiple scales, and metrics for evaluating success or failure.

(2) Risk management: Achieving appropriate levels of security requires more than technology. The application of these technologies requires significant insight into an organization's goals, its abilities and modalities, and the nature of the threats it faces. Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact so they can determine an acceptable level of risk tolerance.

(3) Human aspects: Comprehensive cybersecurity requires understanding the human facets of cyber threats and secure cyber systems.

(4) Transitioning successful research into practice: Federal R&D spending in the cybersecurity arena remains a high national priority and ensuring the transition of research into practice is essential to maximizing return on investments.

(5) Workforce development: Developing and retaining the necessary cybersecurity workforce remains a key challenge. People are an essential component of cyber systems and can contribute to their security (or insecurity) in a variety of ways.

(6) Enhancing the research infrastructure: Access to advanced cybersecurity testbeds continues to be a hurdle for researchers. Testbeds are essential so that researchers can use actual operational data to model and conduct experiments on real-world system vulnerabilities and exploitation scenarios in proper test environments.

The National Science Foundation (NSF) funding programme states in their synopsis[3] that "The goals of the Secure and Trustworthy Cyberspace (SaTC) program are aligned with the Federal Cybersecurity Research and Development Strategic Plan

[2] Federal Cybersecurity Research and Development Strategic Plan https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

[3] National Science Foundation (NSF) synopsis https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709&org=CISE&from=home

(RDSP) and the National Privacy Research Strategy (NPRS) to protect and preserve the growing social and economic benefits of cyber systems while ensuring security and privacy. Therefore, we felt it would be best to segregate the types of R&D being funded by NSF in relation to these critical areas of importance to the national strategy.

However, it was difficult to find any particular activity in relation to critical area (4), transitioning successful research into practice, apart from some activities related to DARPA and DHS. It is unclear whether there is no particular funding mechanism for this kind of research to innovation to market activity, or whether the activities are being disseminated elsewhere. For this critical area, please see section 5, which deals with steps related to the strengthening of the cybersecurity and privacy markets in the US. Therefore, the first set of topics relate to the five critical areas identified by the RDSP.

In addition, we have added a sixth category on Frameworks, to highlight the key activities in relation to Cybersecurity related Frameworks being carried out in the United States.

2.1 Scientific Foundations

2.1.1 Big Data

The National Science Foundation (NSF) is a leader in supporting Big Data research efforts. These efforts are part of a larger portfolio of Data Science activities. NSF initiatives in Big Data and Data Science encompass Research, Cyberinfrastructure, Education and Training, and Community Building[4]. NSF research programs in Big Data cover algorithmic, statistical, and mathematical foundations of data science; new techniques, technologies, and methodologies, including hardware and software approaches; and innovative uses of data for scientific discovery and action. Within Research, there are two programs: 1. **Critical Techniques, Technologies and Methodologies for Advancing Foundations and Applications of Big Data Sciences and Engineering (BIGDATA**[5]). The BIGDATA program seeks novel approaches in computer science, statistics, computational science, and mathematics, along with innovative applications in domain science. 2. **Computational and Data–Enabled Science and Engineering (CDS&**E[6]): The goal of the CDS&E program is to identify and capitalize on opportunities for major scientific and engineering breakthroughs through new computational and data analysis approaches.

In December 2017, members of the Networking and Information Technology Research and Development (NITRD[7]) Program's Cyber Security and Information Assurance Interagency Working Group (CSIA IWG[8]) presented the panel **Big Data for Security - Can We Improve Security and Preserve Privacy?**[9] held during the annual Computer Security Applications Conference. The panel was composed of representatives from Defense Advanced Research Projects Agency (DARPA[10]); NSF; Office of the Assistant Secretary of Defense; Cyber Security Division, Department of Homeland Security S&T; and NITRD. The panellists discussed Federal research to advance the use of big data analytics for security and use of privacy-preserving

[4] https://www.nsf.gov/cise/bigdata/
[5] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504767
[6] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504813
[7] https://www.nitrd.gov/
[8] https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Security_and_Information_Assurance
[9] https://www.nitrd.gov/nitrdgroups/images/5/5c/ACSAC2017_NITRDPanel.pdf
[10] https://www.darpa.mil/

technologies, including attempts to reconcile conflicting objectives. CSIA IWG focus on research and development to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems. These systems provide both the basic infrastructure and advanced communications in every sector of the economy, including critical infrastructures such as power grids, emergency communications systems, financial systems, and air-traffic-control networks. These systems also support national defense, national and homeland security, and other vital Federal missions, and themselves constitute critical elements of the IT infrastructure. Broad areas of concern include Internet and network security; confidentiality, availability, and integrity of information and computer-based systems; new approaches to achieving hardware and software security; testing and assessment of computer-based systems security; and reconstitution and recovery of computer-based systems and data.

2.1.2 Biometrics

Computer data obtained from sensors that identify a person based on unique physical characteristics and traits, such as fingerprints or retinal scans. Unlike passwords, which are based on what a person can remember and thus easier to guess, biometrics are nearly impossible to fool. A team at Texas State University San Marcos are making **ocular biometrics**[11] more secure and reliable.

2.1.3 Differential privacy

This is a method that allows researchers to investigate data without revealing confidential information. Differential privacy provides approximate answers to queries that include enough "noise" so an adversary cannot find out information specific to any individual in the database. NSF supports a team at Harvard University that is putting the concept into practice to **protect sensitive research data**[12].

2.1.4 Hardware security

Processes and tools used to ensure semiconductors are not designed or manufactured in a way that allows them to behave in unintended or malicious ways. **NSF partners with the Semiconductor Research Corporation**[13] to fund research at the circuit, architecture and system levels to decrease unintended behaviour or access, increase resistance to tampering and improve authentication throughout the supply chain.

2.1.5 Heart-scan

A University at Buffalo-led team has developed a computer security system using the dimensions of **heart as identifier**[14]. The system uses low-level Doppler radar to measure your heart, and then continually monitors your heart to make sure no one else has stepped in to run your computer.

2.1.6 Indistinguishability obfuscation

A method that transforms a computer program into a "**multilinear jigsaw puzzle**[15]". Each piece of the program mixes in carefully chosen random elements so that the randomness cancels out and the pieces fit together to compute the

[11] http://www.nsf.gov/news/special_reports/science_nation/eyebiometrics.jsp
[12] http://www.nsf.gov/news/news_summ.jsp?cntn_id=136499
[13] http://www.nsf.gov/news/news_summ.jsp?cntn_id=132795
[14] http://www.buffalo.edu/news/releases/2017/09/034.html
[15] http://web.cs.ucla.edu/cef/

correct output. The idea has the potential to transform cybersecurity and is supported by several NSF grants.

2.1.7 Internet of Things

University of Washington's **Security and Privacy Research Lab**[16] with support from NSF **exposed weaknesses in car computer systems**[17]. Their current interests include the field of "augmented reality," which includes technologies like Google Glass or Microsoft's HoloLens that take computer-generated information including graphics, sound or videos and projects it into a real-world setting. In February, 2018, NIST released the **Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things**[18] **(IoT) (Draft NISTIR 8200).** This report is described later in section 2.6.1.

2.1.8 Keys (public key encryption)

A piece of information that specifies the particular transformation of plain text into ciphertext, or vice versa, used for encryption and decryption. In the 1970s, researchers supported by NSF invented "**public key**[19]" cryptographic algorithms that became a critical piece of the Internet's cybersecurity infrastructure.

2.1.9 Medical device security

Medical applications offer tremendous opportunities to improve individual wellness and public health, but are often not designed with security and privacy in mind. Researchers from Dartmouth, Johns Hopkins, and the University of Michigan are collaborating on the **Trustworthy Health and Wellness project**[20] to develop mobile- and cloud-computing systems that respect the privacy of individuals and the trustworthiness of medical information.

2.1.10 Networks, Mobile

Increasingly, people are relying on their phones or other mobile devices, rather than computers, for Internet service. Those devices are convenient, but come with a host of security issues. NSF's collaborative **Future Internet Architecture's Next-Phase**[21] grants seek to enhance security in these new network architectures.

Through its **Beyond Today's Internet initiative**[22]**,** NSF's investments in novel hardware and software, and new networking architectures, protocols and applications have enhanced the speed, security and accessibility of the Internet. Being conscious that the Internet is a critical infrastructure now and for the future, and that it is not a solved problem, NSF supports research on all aspects of the **Next Generation Internet (NGI**[23]**)**.

In this context, NSF/Directorate for **Computer and Information Science and Engineering (CISE)** and the European Commission's **DG CONNECT** recognized the opportunity for the US and EU to jointly benefit from international research collaborations in NGI and Advanced Wireless Networking (AWN) systems and technologies, which will accelerate the creation of a global, human-centric internet. To that end, NSF/CISE has recently launched the **US-EU Internet Core & Edge**

[16] https://seclab.cs.washington.edu/
[17] http://www.autosec.org/pubs/cars-oakland2010.pdf
[18] https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf
[19] https://people.csail.mit.edu/rivest/Rsapaper.pdf
[20] https://thaw.org/about/
[21] http://www.nsf.gov/news/news_summ.jsp?cntn_id=131248
[22] Beyond Today's Internet initiative https://www.nsf.gov/news/special_reports/ignite/
[23] http://www.ngi.eu/

Technologies (ICE-T) Program Awards for US investigators to collaborative research with EU investigators in NGI and AWN[24] that is expected to align with the related efforts in the NGI initiative in the EC's Horizon 2020's Work Programme for 2018-2020.

2.1.11 Network Traffic Analysis

By analysing network traffic going to suspicious domains, security administrators could detect malware infections weeks or even months before they're able to capture a sample of the invading malware, suggested by the NSF supported research at Georgia Tech. The findings point toward the need for new malware-independent detection strategies that will give network defenders the ability to identify network security breaches in a timelier manner.

2.1.12 Open source cybersecurity software

Cybersecurity software that is given away freely and that allows users to change its code to suit their purposes. The **Department of Homeland Security and the National Security Agency** [25] have both embarked on efforts to assess the usefulness of such tools for cybersecurity and to release open source tools to the public. The NSF-supported **Bro Network Security Monitor**[26] is an example of open source security software available for public use.

2.1.13 Quantum cryptography

The use of the quantum mechanical properties of photons to perform cryptographic tasks that are believed to be impossible using only classical computing methods. NSF-supported researchers are designing a quantum cryptography protocol[27] for securing optical burst switching networks.

2.1.14 Ransomware Payments

The murky ecosystem of ransomware payments has been the focus of NSF assisted university and industry researchers. It aims to provide a first detailed account of the ransomware payment ecosystem, from initial attack to cash-out. Ransomware attacks, which encrypt and hold a computer user's files hostage in exchange for payment, extort millions of dollars from individuals each month, and comprise one of the fastest-growing forms of cyberattack.

2.1.15 Zombie cyber-attacks

Spam and denial-of-service attacks coming from compromised computers (zombies) that have been infected with malware and are now controlled remotely by the attacker. NSF is supporting researchers who are developing methods to **detect zombie cyber-attacks**[28] on a network and prevent future attacks.

[24] NSF's ICE-T Program Solicitation NSF 18-535. https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505516&WT.mc_id=USNSF_39&WT.mc_ev=click
[25] http://www.livescience.com/14356-cybersecurity-open-source.html
[26] https://www.bro.org/
[27] http://nsf.gov/awardsearch/showAward?AWD_ID=1117179&HistoricalAwards=false
[28] http://nsf.gov/awardsearch/showAward?AWD_ID=1041739&HistoricalAwards=false

2.2 Risk Management

2.2.1 Forensics

Methods to understand what happened after a security incident to assure attacks aren't repeated. Tools like the **Bro Network Security Monitor**[29], funded by NSF, let experts perform complex cyber-forensics to study the patterns of attacks, assess the damage and design better ways to block them in the future. Separately, faculty at Metropolitan State University and the University of Minnesota are exploring the use of **augmented reality for cybersecurity forensics education**[30].

2.2.2 Governance

The common rules, policies and procedures that allow the Internet to function. Governance ensures that participating entities use interoperable systems and technologies, and ensures that unique identifiers, like domain names, aren't used by multiple parties. For decades, NSF research has helped stakeholders shape governance as the Internet developed; **governance issues remain a major area of today's NSF-supported work**[31].

2.2.3 Risk assessment

Improving cybersecurity by modelling and assessing real-world risks and developing risk mitigation methods to limit vulnerabilities. With NSF support, researchers from Iowa State have been applying this method **to attacks on our electric power infrastructure**[32]. Within this space, researchers from `University of Illinois at Urbana-Champaign, Michigan at Ann Arbor and California at Berkeley are working on **large collaborative Internet-Wide Vulnerability Measurement, Assessment, and Notification**[33]. Recent advances in Internet-wide scanning make it possible to conduct network surveys of the full public IPv4 address space in minutes. Thereafter when new vulnerabilities are announced, the Internet security community can comprehensively identify the systems that suffer from these vulnerabilities and automatically take steps to help affected system operators correct the problems.

2.2.4 Law

Cybersecurity laws help protect our security and privacy, but there are trade-offs when engaging in cyber offense and defense. A more secure Internet encourages participation online and reduces citizens' exposure to cybercrime, but limits governments' ability to gain intelligence and strategic advantage. With NSF funding, researchers from the University of Tulsa are **constructing a taxonomy of offensive and defensive cyber-attack options**[34] and the possible collateral damage they may cause, helping policymakers assess the value of cyber operations against the unintended consequences.

2.2.5 Social media analysis

Social media communications can yield enormous amounts of data about communities – including hackers and cybercriminals. With NSF support, researchers at the University of Arizona are studying those social media channels to learn about **hacker behaviours, markets, community structures and cultural**

[29] http://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=135868
[30] http://www.nsf.gov/awardsearch/showAward?AWD_ID=1500055&HistoricalAwards=false
[31] http://www.nsf.gov/awardsearch/showAward?AWD_ID=1540066&HistoricalAwards=false
[32] http://www.nsf.gov/awardsearch/showAward?AWD_ID=0915945&HistoricalAwards=false
[33] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1518921&HistoricalAwards=false
[34] http://nsf.gov/awardsearch/showAward?AWD_ID=1444863&HistoricalAwards=false

differences[35]. Researchers at Carnegie-Mellon University are testing to see if "nudges[36]" on social media can be used to encourage users towards safer behaviors.

2.2.6 Insider Threats

Researchers at the State University of New York at Buffalo are working to help organizations map out the spots most vulnerable to insiders and, eventually, develop countermeasures aimed directly at those threats. With support from the National Science Foundation's Secure and Trustworthy Cyberspace (SaTC) initiative, they are conducting one of the first large-scale studies of **how insiders behave on a network**[37] that allows them to view sensitive information.

2.3 Human Aspects

2.3.1 Cryptocurrency

A new form of digital currency where encryption techniques are used to regulate the generation of currency and verify its transfer, independent of a central bank. A new project supported by NSF with researchers at the University of Maryland, UC Berkeley and Princeton aims to establish a rigorous **scientific foundation for crypto-currencies**[38].

2.3.2 Anti-censorship

Methods for combatting censorship by developing accurate models of the capabilities of censors – for example blocked search results or interference with international network traffic – as well as how those capabilities will likely evolve. An NSF-funded team from UC Berkeley, Georgia Tech, the University of New Mexico is working to develop the **science of censorship resistance**[39].

2.3.3 Power grid security

The electric power grid is a complex cyber-physical system with possible associated cybersecurity risks. Engineers are developing new protective countermeasures based on innovative algorithmic tools to **detect**[40] and mitigate[41] cyber intrusions before they disrupt critical systems, with work previously done in this space also on **securing smart electricity meters**[42].

2.3.4 Usability

Security features of digital environments can make them easier or harder to use. Poor usability translates into inadequate protection, thereby limiting the effectiveness of such features. Tools developed by researchers at Carnegie Mellon University **extract key privacy policy features**[43] from website privacy policies and present these features to users in an easy-to-digest format. The tools enable individuals to make more informed privacy decisions as they interact with different websites.

[35] http://www.nsf.gov/awardsearch/showAward?AWD_ID=1314631&HistoricalAwards=false
[36] http://yangwang.syr.edu/papers/CHI2014.pdf
[37] https://nsf.gov/awardsearch/showAward?AWD_ID=1420758
[38] http://nsf.gov/awardsearch/showAward?AWD_ID=1518765&HistoricalAwards=false
[39] http://nsf.gov/awardsearch/showAward?AWD_ID=1518918&HistoricalAwards=false
[40] http://www.nsf.gov/awardsearch/showAward?AWD_ID=1351621&HistoricalAwards=false
[41] http://www.nsf.gov/awardsearch/showAward?AWD_ID=1151076&HistoricalAwards=false
[42] https://nsf.gov/discoveries/disc_summ.jsp?cntn_id=136484&org=NSF&from=news
[43] http://www.usableprivacy.org/

2.3.5 Voting security

Cybersecurity systems designed to ensure that electronic voting machines cannot be tampered with and that records remain private. With input from stakeholders such as local election officials and voters, researchers from Rice University are constructing a **prototype voting system**[44] that is significantly more secure than current solutions, and at the same time makes it easier to participate in the election process.

2.3.6 XRay

A personal data tracking tool for the Web that predicts which data in one's Web accounts -- such as emails, searches, or viewed products – is being used to generate targeted ads, recommended products or personalized prices. Developed by a team at Columbia University, the **XRay**[45] tool compares outputs from different accounts with similar, but not identical, subsets of data, to pinpoint targeting through correlation. The tool addresses the limited visibility we have into how our data is being used.

2.3.7 Your personal data

Personal data breaches have become parts of daily life. But do people change habits or behave any differently after receiving data breach notifications from banks or retailers? Researchers at Carnegie Mellon University, with NSF support, are asking questions that could help companies **fine-tune their data breach notifications**[46].

2.3.8 Health

With Internet-connected medical technology and digitized health records on the rise, cybersecurity is a growing concern for patients and hospitals alike. One research team is taking a holistic approach to strengthening the medical system's security -- from the computer networks that support hospitals, to the cloud, to the smart phone in your pocket. A National Science Foundation (NSF)-funded project, titled "Trustworthy Health and Wellness" (THaW.org) aims to protect patients and preserve the confidentiality of medical data as records move from paper to electronic form. THaW researchers conducted **three studies of the mHealth apps**[47] in Google Play to determine how common apps handle medical data. They found a variety of vulnerabilities that a malicious party could exploit to gain access to sensitive data. Perhaps more significantly, they found that many apps send sensitive information over the Internet in ways that are fundamentally insecure. This lack of security is not limited to mHealth apps. The researchers found critical vulnerabilities in some health care environments as well, like hospitals, where workstations used by clinicians can be susceptible to unwarranted access. Hospital workstations allow doctors to enter information about patients efficiently, without having to transcribe notes or return to their offices. But user authentication at those terminals requires time and effort from clinicians - they have to log in, then remember to log out. Because of these inconveniences, doctors sometimes do not log out, leaving computers unsecured and open to use by other parties. The BRACE (Bilateral Recurring Authentication Conducted Effortlessly) project addresses this challenge by developing a user-friendly authentication mechanism that blends seamlessly into the clinicians' workflow.

[44] http://discovermagazine.com/2014/julyaug/1-lock-the-vote
[45] http://columbia.github.io/xray/
[46] http://www.nsf.gov/awardsearch/showAward?AWD_ID=1359632
[47] http://seclab.illinois.edu/wp-content/uploads/2014/08/HeNGN14.pdf

2.4 Workforce development

2.4.1 Education, cybersecurity

Training to ensure that ethical cybersecurity experts are available for service in government and industry. NSF funds basic research in cybersecurity together with research on learning, as well as a number of **cybersecurity education programs**[48], to address this challenge.

2.4.2 Jobs, cybersecurity

Protecting cyberspace requires a **cybersecurity workforce**[49] that can rapidly detect and respond to threats and create ways to thwart attacks by design before they occur. More than ten thousand cybersecurity workers are needed by the government and many more are required by industry.

2.4.3 White hat hackers

An ethical computer hacker, known as a "white hat", who specializes in authorized testing of networks and software to ensure the security of an organization's information systems. Every year, through the **CyberCorps: Scholarship for Service**[50] program, **NSF trains hundreds of experts**[51], whose skills include ethical hacking and places them in positions within the government.

2.5 Enhancing the research infrastructure

2.5.1 Testbeds

Experimental research infrastructures that help cybersecurity experts understand risks before they become problems. Testbeds may be for generalized use, like the **DETER**[52] Project, or highly specialized, such as certain cyber physical testbeds. They may include specific physical apparatus, hardware tools, and simulators, and should integrate live and synthetic humans, as well as capabilities to ensure scientific validity. NSF recently funded a **study**[53]**to develop a roadmap for future cybersecurity experimentation.**

2.5.2 Cybersecurity Innovation for Cyberinfrastructure (CICI)

The objective of the Cybersecurity Innovation for Cyberinfrastructure (CICI) program is to develop, deploy and integrate security solutions that benefit the scientific community by ensuring the integrity, resilience and reliability of the end-to-end scientific workflow. CICI seeks three categories of projects- Secure Scientific Cyberinfrastructure, Collaborative Security Response Centre and Research Data Protection. A sample of recent CICI awards is shown here for information purposes and the full list of awards made through this program can be found **here**[54].

[48] https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW_FinalReport_040714.pdf
[49] http://nsf.gov/discoveries/disc_summ.jsp?cntn_id=133185&org=NSF
[50] https://www.sfs.opm.gov/
[51] http://nsf.gov/discoveries/disc_summ.jsp?cntn_id=133185&org=NSF
[52] http://deter-project.org/about_deter_project
[53] http://cyberexperimentation.org/files/5514/3834/3934/CEF_Final_Report_20150731.pdf
[54] https://www.nsf.gov/awardsearch/advancedSearchResult?ProgEleCode=8027&BooleanElement=Any&BooleanRef=Any&ActiveAwards=true&#results

Collaborative Research: CICI: Regional: SouthEast SciEntific Cybersecurity for University Research (SouthEast SECURE)[55]
Award Number:1812404; Principal Investigator:Anthony Skjellum; Co-Principal Investigator:; Organization:University of Tennessee Chattanooga;NSF Organization:OAC Start Date:10/01/2017; Award Amount:$76,949.00; Relevance:48.0;

CICI: RSARC: DDoS Defense In Depth for DNS[56]
Award Number:1739034; Principal Investigator:John Heidemann; Co-Principal Investigator:Jelena Mirkovic, Wes Hardaker; Organization:University of Southern California;NSF Organization:OAC Start Date:10/01/2017; Award Amount:$997,226.00; Relevance:48.0;

CICI: CE: Enhancing Cybersecurity for Broadening Data-Driven Research and Partnerships[57]
Award Number:1738981; Principal Investigator:Sonia Fahmy; Co-Principal Investigator:Xiao Zhu, Ida Ngambeki, Nicole Key, Bruno Ribeiro; Organization:Purdue University;NSF Organization:OAC Start Date:10/01/2017; Award Amount:$841,506.00; Relevance:48.0;

CICI: CE: Improving the Security of a Science DMZ[58]
Award Number:1739025; Principal Investigator:Matt Bishop; Co-Principal Investigator:Dipak Ghosal, Viji Murali; Organization:University of California-Davis;NSF Organization:OAC Start Date:10/01/2017; Award Amount:$738,094.00; Relevance:48.0;

CICI: CE: Implementing CYBEX-P: Helping Organizations to Share with Privacy Preservation[59]
Award Number:1739032; Principal Investigator:Shamik Sengupta; Co-Principal Investigator:Mehmet Gunes, Nancy LaTourrette, Ming Li, Jeff Springer; Organization:Board of Regents, NSHE, obo University of Nevada, Reno;NSF Organization:OAC Start Date:01/01/2018; Award Amount:$1,002,067.00; Relevance:48.0.

2.6 Framework Activities

2.6.1 National Institute of Standards and Technology (NIST)

There are a number of ongoing activities in the US in relation to the development of the technological aspects pertaining to the cybersecurity of critical infrastructures. One of the most prominent is the **Cybersecurity Framework** [60] under development by the National Institute of Standards and Technology (NIST). NIST is a federal agency within the United States Department of Commerce, whose mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST is also responsible for establishing computer- and information technology-related standards and guidelines for federal agencies to use. Many private sector organizations have made widespread use of these standards and guidelines voluntarily for several decades, especially those related to information security.

[55] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1812404&HistoricalAwards=false
[56] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1739034&HistoricalAwards=false
[57] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1738981&HistoricalAwards=false
[58] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1739025&HistoricalAwards=false
[59] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1739032&HistoricalAwards=false
[60] https://www.nist.gov/cyberframework

Version 1.0 of the Framework was prepared by NIST with extensive private sector input and issued in February 2014. The Framework was developed in response to **Presidential Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity** [2], which was issued in 2013 by President Barack Obama. Among other things, the EO directed NIST to work with industry leaders to develop the Framework. The Framework was developed in a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders. That took place via workshops, extensive outreach and consultation, and a public comment process. NIST's future Framework role is reinforced by the Cybersecurity Enhancement Act of 2014 (Public Law 113-274), which calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure. This collaboration continues as NIST works with stakeholders from across the country and around the world to raise awareness and encourage use of the Framework.

The most recent version, Framework V1.1 [3] was released on April 16, 2018, following a 45-day public comment period on the second draft of Framework V1.1.This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. According to the NIST web site, Version 1.1 has evolved to be even more informative, useful, and inclusive for all kinds of organizations. It is fully compatible with Version 1.0 and remains flexible, voluntary, and cost-effective. A summary of the updates to V1.1 include: Declares applicability of the Framework for "technology," which is minimally composed of information technology, operational technology, cyber-physical systems, and Internet of Things; Enhances guidance for applying the Framework to supply chain risk management; Summarizes the relevance and utility of Framework measurement for organizational self-assessment; Better accounts for authorization, authentication, and identity proofing, and Administratively updates the Informative References. For a more detailed analysis of V1.1 updates, a Cybersecurity Framework V1.1 Overview webcast is available at https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview .

The NIST Cybersecurity Framework is applicable to many different technologies, including Internet of Things (IoT) technologies. The view was taken that developing separate frameworks of cybersecurity outcomes specific to IoT might risk losing a critical mass of users aligning their cybersecurity outcomes to Cybersecurity Framework. Therefore, to retain that alignment, NIST recommends continued evaluation and evolution of the Cybersecurity Framework to make it even more meaningful to IoT technologies. NIST welcomes observations from all parties regarding Cybersecurity Framework's relevance to IoT, and these will be vetted with the NIST Cybersecurity for IoT Program[61].

While the Framework was borne through U.S. policy, NIST emphasises that it is not a "U.S. only" Framework. The private sector stakeholders involved made it clear from the outset that global alignment is important to avoid confusion and duplication of effort, or even conflicting expectations in the global business environment. These needs have been reiterated by multi-national organizations. The importance of international standards organizations and trade associations for acceptance of the Framework's approach has been widely recognized. Some countries and international entities are adopting approaches that are compatible with the framework established by NIST, and others are considering doing the same. NIST has been holding regular discussions with many nations and regions,

[61] https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

and making noteworthy internationalization progress. NIST is actively engaged with international standards-developing organizations to promote adoption of approaches consistent with the Framework.

In terms of updates, as the Framework was always meant to be a "living document", it is expected there will be more updates in the future of the Framework to keep pace with technology and threat trends, integrate lessons learned, and establish best practice as common practice. The development of proposed updates and finalization of those updates into new versions of the Framework is and will be done in coordination with the NIST stakeholders and in consultation with the parties outlined in the Cybersecurity Enhancement Act of 2014 [4].

NIST also coordinates the **Cyber-Physical Systems (CPS) Framework**[62], which includes a structure and analysis methodology for CPS. The goal of the CPS Framework is to develop a shared understanding of CPS, its foundational concepts and unique dimensions, promoting progress through the exchange of ideas and integration of research across sectors and to support development of CPS with new functionalities. It is recognised that the impacts of CPS will be revolutionary and pervasive, which is evident today in emerging smart cars, intelligent buildings, robots, unmanned vehicles, and medical devices. Realizing the future promise of CPS will require interoperability between elements and systems, supported by new reference architectures and common definitions and lexicons. Addressing the problems and opportunities of CPS requires broad collaboration to develop a consensus around these concepts, and a shared understanding of the essential roles of timing and cybersecurity. To this end, NIST has established the CPS Public Working Group (CPS PWG[63]), which is open to all, to foster and capture inputs from those involved in CPS, both nationally and globally. As part of this, there is a working group dedicated to developing a cybersecurity and privacy strategy for the common elements of CPS. This includes identification, implementation, and monitoring of specific cybersecurity activities (including the identification, protection, detection, response and recovery of CPS elements) and outcomes for CPS in the context of a risk management program. Where applicable standards, guidelines, and measurement metrics do not exist, this working group will identify areas for further CPS cybersecurity research and development.

NIST also coordinated the **Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things**[64] **(IoT) (Draft NISTIR 8200),** released in February, 2018. The report was prepared by the Interagency International Cybersecurity Standardization Working Group (IICS WG[65]), which was established in December 2015, by the National Security Council's Cyber Interagency Policy Committee (NSC Cyber IPC). Its purpose is to coordinate on major issues in international cybersecurity standardization and thereby enhance U.S. federal agency participation in international cybersecurity standardization. On April 25, 2107, the IICS WG established an Internet of Things (IoT) Task Group to determine the current state of international cybersecurity standards development for IoT. This Report is intended for use by the IICS WG member agencies to assist them in their standards planning and to help to coordinate U.S. government participation in international cybersecurity standardization for IoT.

[62] https://www.nist.gov/el/cyber-physical-systems
[63] https://pages.nist.gov/cpspwg/
[64] https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf
[65] https://csrc.nist.gov/publications/detail/nistir/8200/draft

2.6.2 Department of Homeland Security

Presidential Executive Order (EO) 1363 also charged the Department of Homeland Security (DHS[66]) with developing a voluntary program to promote use of the Framework and help critical infrastructure organizations improve their cybersecurity. In February 2014, DHS launched the **Critical Infrastructure Cyber Community (C3, pronounced "C-Cubed") Voluntary Program**. The C3 Voluntary Program helps align critical infrastructure owners and operators with existing resources to assist in their efforts to use the Framework and manage their cybersecurity risks. More information about the C3 Voluntary Program may be found at https://www.us-cert.gov/ccubedvp.

The United States Computer Emergency Readiness Scheme (US-CERT), which is part of the Department of Homeland Security, hosts the National Cybersecurity and Communications Integration Center (NCCIC[67]). NCCIC is the US's flagship cyber defense, incident response, and operational integration center, whose mission is to reduce the Nation's risk of systemic cybersecurity and communications challenges. Since 2009, NCCIC has served as a national hub for cyber and communications information, technical expertise, and operational integration, and by operating 24/7 situational awareness, analysis, and incident response center.

It was announced in a press release[68] on 12th July, 2018 that small businesses in the research and development domain will have the opportunity to engage with the U.S. Department of Homeland Security's Small Business Innovation Research (SBIR) program representatives beginning July 17th, as part of the third of four legs of a National Road Tour sponsored by the Small Business Administration.

"The SBIR Road Tour continues to be a great way to discuss opportunities for innovative small businesses to engage on technology needs for the Homeland Security mission," said William N. Bryan, DHS Senior Official Performing the Duties of the Under Secretary for Science and Technology. "By participating in this road tour and engaging with small businesses we facilitate the development of new technologies for the homeland security enterprise and support small business as a driving force for the US economy."

The Road Tour is a national outreach effort that connects small businesses with funding opportunities provided through the SBIR/STTR programs. Small businesses in the innovation research and development domains are encouraged to participate in this opportunity to meet DHS SBIR Program representatives and learn how to help address the homeland security challenges facing the nation.

[66] https://www.dhs.gov/
[67] https://www.us-cert.gov/
[68] https://www.dhs.gov/science-and-technology/news/2018/07/12/news-release-dhs-engage-innovative-sb-pacific-northwest

2.6.3 Defense Advanced Research Projects Agency (DARPA)

For sixty years, DARPA[69] has held to a singular and enduring mission: to make pivotal investments in breakthrough technologies for national security.

The genesis of that mission and of DARPA itself dates to the launch of Sputnik in 1957, and a commitment by the United States that, from that time forward, it would be the initiator and not the victim of strategic technological surprises. Working with innovators inside and outside of government, DARPA has repeatedly delivered on that mission, transforming revolutionary concepts and even seeming impossibilities into practical capabilities. The ultimate results have included not only game-changing military capabilities such as precision weapons and stealth technology, but also such icons of modern civilian society such as the Internet, automated voice recognition and language translation, and Global Positioning System receivers small enough to embed in myriad consumer devices.

DARPA explicitly reaches for transformational change instead of incremental advances. But it does not perform its engineering alchemy in isolation. It works within an innovation ecosystem that includes academic, corporate and governmental partners, with a constant focus on the Nation's military Services, which work with DARPA to create new strategic opportunities and novel tactical options. For decades, this vibrant, interlocking ecosystem of diverse collaborators has proven to be a nurturing environment for the intense creativity that DARPA is designed to cultivate.

DARPA comprises approximately 220 government employees in six technical offices, including nearly 100 program managers, who together oversee about 250 research and development programs.

[69] https://www.darpa.mil/

3 US CYBERSECURITY AND PRIVACY STRATEGY

The current U.S. cybersecurity strategy focuses on four well-defined strategic pillars[70]:

I. Protect the homeland, the American people, and American way of life;
II. Promote American prosperity;
III. Preserve peace through strength;
IV. Advance American influence.

Each of these pillars is clearly outlined by President Donald Trump in the "National Security Strategy" through which he provided some high-level lines of action. This document describes the main objectives of this strategy, including the role of the Internet and information technology as a relevant element in a defensive perspective.

The first three pillars are particularly focused on the issues of cybersecurity. The White House shows how cyberspace is now a fundamental part of every aspect of national security.

Another fundamental objective of the new U.S. strategy also includes topics, such as protection and resilience of national critical infrastructures from cyber- attacks. In order to accomplish, President Trump's line is to pay particular attention to real risks, which cover the following critical areas of intervention: national security, energy, banking and finance, health and safety, communications and transport. The main purpose is to identify where and how cyber-attacks could occur and ensure high priority interventions in these areas in terms of support, capacity building, and defense.

The United States Cybersecurity and Privacy strategy can be broken into the national (federal) strategy and an international strategy, through a relatively small number of instruments (i.e. Strategic Plans).

3.1 Federal Cybersecurity Research and Development Strategic Plan

The National Science and Technology Council's (NSTC[71])'s Federal Cybersecurity Research and Development Strategic Plan [1] responds to Section 201 of the Cybersecurity Enhancement Act of 2014 [2], which directs the NSTC and the Networking and Information Technology Research and Development (NITRD[72]) Program to develop a strategic plan to guide Federal cybersecurity research and development. It builds on Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, which was released by the NSTC in December 2011.

Before going into detail about the strategic plan itself, we will outline the different stakeholders involved in the plan.

The **National Science and Technology Council** (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development (R&D) enterprise. One of the NSTC's primary objectives is establishing clear national goals

[70] https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-announces-national-security-strategy-advance-americas-interests/
[71] https://www.whitehouse.gov/ostp/nstc/
[72] https://www.nitrd.gov/

for Federal science and technology investments. The NSTC prepares R&D packages aimed at accomplishing multiple national goals. The NSTC's work is organized under five committees: Environment, Natural Resources, and Sustainability; Homeland and National Security; Science, Technology, Engineering, and Mathematics (STEM) Education; Science; and Technology. Each of these committees oversees subcommittees and working groups that are focused on different aspects of science and technology. More information is available at www.whitehouse.gov/ostp/nstc.

The **Office of Science and Technology Policy** (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976. OSTP's responsibilities include advising the President in policy formulation and budget development on questions in which science and technology are important elements; articulating the President's science and technology policy and programs; and fostering strong partnerships among Federal, state, and local governments, and the scientific communities in industry and academia. The Director of OSTP also serves as Assistant to the President for Science and Technology and manages the NSTC. More information is available at www.whitehouse.gov/ostp.

The **Subcommittee on Networking and Information Technology Research and Development** (NITRD), also known as the NITRD Program, is a body under the Committee on Technology (CoT) of the NSTC. The NITRD Subcommittee coordinates multi-agency research and development programs to help assure continued U.S. leadership in networking and information technology, satisfy the needs of the Federal Government for advanced networking and information technology, and accelerate development and deployment of advanced networking and information technology. It also implements relevant provisions of the High-Performance Computing Act of 1991 (P.L. 102-194), as amended by the Next Generation Internet Research Act of 1998 (P.L. 105-305), and the America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education and Science (COMPETES) Act of 2007 (P.L. 110-69). For more information, see www.nitrd.gov.

The Federal Cybersecurity Research and Development Strategic Plan (2016) updates and expands the December 2011 plan, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* [5], which defined a set of interrelated breakthrough objectives for Federal agencies that conduct or sponsor R&D in cybersecurity. This Plan incorporates and expands the priorities in the 2011 plan and adds a strong focus on evidence validated R&D. Evidence of cybersecurity efficacy and efficiency, such as formal proofs and empirical measurements, drives progress in cybersecurity R&D and improves cybersecurity practice.

Four assumptions are the foundation of this plan:

1. **Adversaries.** Adversaries will perform malicious cyber activities as long as they perceive that the potential results outweigh the likely effort and possible consequences for themselves.
2. **Defenders.** Defenders must thwart malicious cyber activities on increasingly valuable and critical systems with limited resources and despite evolving technologies and threat scenarios.
3. **Users.** Users—legitimate individuals and enterprises2—will circumvent cybersecurity practices that they perceive as irrelevant, ineffective, inefficient, or overly burdensome.
4. **Technology.** As technology cross-connects the physical and cyber worlds, the risks as well as the benefits of the two worlds are interconnected.

The plan defines three research and development goals to provide the science, engineering, mathematics, and technology necessary to improve cybersecurity in

light of these assumptions. The science and engineering advances needed are socio-technical in nature, and vary from foundational to applied over a range of time scales[73]:

> **Near-Term Goal** (1-3 years). Achieve S&T advances to counter adversaries' asymmetrical advantages with effective and efficient risk management.
>
> **Mid-Term Goal** (3-7 Years). Achieve S&T advances to reverse adversaries' asymmetrical advantages, through sustainably secure systems development and operation.
>
> **Long-Term Goal** (7-15 years). Achieve S&T advances for effective and efficient deterrence of malicious cyber activities via denial of results and likely attribution.

To achieve these goals, the Plan focuses on developing S&T to support four defensive elements:

1. **Deter.** The ability to efficiently discourage malicious cyber activities by measuring and increasing costs to adversaries carrying out such activities, diminishing the spoils, and increasing risks and uncertainty for potential adversaries.
2. **Protect.** The ability of components, systems, users, and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability, and accountability.
3. **Detect.** The ability to efficiently detect, and even anticipate, adversary decisions and activities, given that perfect security is not possible and systems should be assumed to be vulnerable to malicious cyber activities.
4. **Adapt.** The ability of defenders, defenses, and infrastructure to dynamically adapt to malicious cyber activities, by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration, and adjusting to thwart similar future activity.

After a description of each element and associated research challenges, the Strategic Plan identifies research objectives to achieve in each element over the near-, mid-, and long-term. he objectives are not comprehensive but establish a basis to measure progress in implementing the Plan. These elements are applicable throughout cyberspace, although some objectives are most meaningful in particular contexts, such as cloud computing or the Internet of Things (IoT).

The Plan identifies six areas critical to successful cybersecurity R&D: (1) scientific foundations; (2) enhancements in risk management; (3) human aspects; (4) transitioning successful research into pervasive use; (5) workforce development; and (6) enhancing the infrastructure for research.

The Plan closes with five core recommendations:

Recommendation 1. Prioritize basic and long-term research in Federal cybersecurity R&D.

Recommendation 2. Lower barriers and strengthen incentives for public and private organizations that would broaden participation in cybersecurity R&D.

Recommendation 3. Assess barriers and identify incentives that could accelerate the transition of evidence-validated effective and efficient cybersecurity research results into adopted technologies, especially for emerging technologies and threats.

[73] "Socio-technical" refers to the human and social factors in the creation and use of technology. For cybersecurity, a sociotechnical approach considers human, social, organizational, economic and technical factors, and the complex interaction among them in the creation, maintenance, and operation of secure systems and infrastructure.

Recommendation 4. Expand the diversity of expertise in the cybersecurity research community.

Recommendation 5. Expand diversity in the cybersecurity workplace. Implementing the Plan and these recommendations will create S&T for cybersecurity that effectively and efficiently defends cyberspace and sustains an Internet that is inherently more secure.

3.2 National Privacy Research Strategy (NPRS)

The National Science and Technology Council's (NSTC's) *National Privacy Research Strategy* (NPRS) [6], developed by the Networking and Information Technology Research and Development (NITRD) Program, was developed in light of the US government's recognition of the challenges to personal privacy from large-scale deployment of information technology systems and from the challenges presented by "Big Data."

The strategy responds to the 2014 reports, Big Data: Seizing Opportunities, Preserving Values [7] by the White House and Big Data and Privacy: A Technological Perspective [8] by the President's Council of Advisors on Science and Technology (PCAST). This strategy establishes objectives and priorities for Federally-funded privacy research, provides a framework for coordinating privacy research and development, and encourages multidisciplinary research that recognizes privacy needs of individuals and society and the responsibilities of the government.

The National Privacy Research Strategy establishes objectives for Federally-funded privacy research (both extramural and government-internal research), provides a structure for coordinating research and development in privacy-enhancing technologies, and encourages multi-disciplinary research that recognizes the responsibilities of the government and the needs of society. The overarching goal of this strategy is to produce knowledge and technology that will enable individuals, commercial entities, and the government to benefit from transformative technological advancements, enhance opportunities for innovation, and provide meaningful protections for personal information and individual privacy.

To achieve these goals, the National Privacy Research Strategy identifies the following priorities for privacy research in the United States:

- Foster multidisciplinary approach to privacy research and solutions;
- Understand and measure privacy desires and impacts;
- Develop system design methods that incorporate privacy desires, requirements, and controls;
- Increase transparency of data collection, sharing, use, and retention;
- Assure that information flows and use are consistent with privacy rules;
- Develop approaches for remediation and recovery; and
- Reduce privacy risks of analytical algorithms.

In May 2017, members of the NITRD's Privacy Research & Development Interagency Working Group (Privacy R&D IWG [74]) led panel discussions on "Research Directions for Federal Privacy R&D" at the 38th IEEE Symposium on Security and Privacy[75] about research problems that should be tackled to achieve the objectives outlined in the (NSTC's) *National Privacy Research Strategy* (NPRS) [6].

[74] https://www.nitrd.gov/nitrdgroups/index.php?title=PrivacyRD
[75] https://www.ieee-security.org/TC/SP2017/program.html

3.3 International Strategy for Cyberspace

The US released its first International Strategy for Cyberspace under President Barack Obama in 2011 [9]. It was the first time any presidential administration had published its vision and goals for cyberspace and cybersecurity. The strategy included several policy initiatives, which the Obama Administration described as "action lines of our strategic framework," and included the following:

- Promoting international standards and innovative, open markets;
- Protecting US networks by enhancing security, reliability and resiliency;
- Extending collaboration with international law enforcement and extending the rule of law;
- Preparing the military for 21st century security challenges;
- Promoting effective and inclusive internet governance structures;
- Working on international development by building capacity, security and prosperity;
- Supporting fundamental internet freedom and privacy.

The Obama Administration also outlined its cybersecurity priorities, areas in which it acted through Presidential Executive Orders and Presidential Directives. The Administration´s priorities on cybersecurity were the following (additional details of these Orders and Directives will be provided in section 4):

- Protecting the nation´s critical infrastructure from cyber threats;
- Improving the nation´s ability to identify and report cyber incidents in a timely manner;
- Engaging with international partners to promote internet freedom and build support for an open interoperable, secure and reliable cyberspace;
- Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets;
- Creating a cyber-savvy workforce.

The US Congress has also acted on presidential cybersecurity priorities by passing laws, including the **Cybersecurity Information Sharing Act** (**CISA**[76]). These legislation elements are described in more detail in section 4.2.

In 2017, President Donald Trump signed **Presidential Executive Order 13800** [10], "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The EO aims to increase the cybersecurity of federal networks, improve cybersecurity of the nation´s critical infrastructure and improve the nation´s overall cybersecurity by: engaging with international allies; ensuring the nation has strategic options to deter adversaries; and training a cybersecurity workforce.

[76] https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf

4 POLICIES AND LEGISLATIONS

4.1 Policy Overview

The following section contains a Cybersecurity policy overview of the United States since 2015.

1. **Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing[77]."** February 13, 2015. This EO promoted the creation of entities such as Information Sharing and Analysis Organizations (ISAOs) that enable businesses, government agencies, and other organizations to share cybersecurity information with each other.

2. **"FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity[78]."** June 12, 2015. This effort, better known as the 30-Day Cybersecurity Sprint, directed federal agencies to make several immediate improvements to their cybersecurity policies and processes. It also formed a Cybersecurity Sprint Team to review federal cybersecurity policies and processes, identify shortcomings and priorities, and recommend how to address them. In addition, the Sprint directed the development of a federal cybersecurity strategy based on the following key principles:

   a. protecting data;
   b. improving situational awareness;
   c. increasing cybersecurity proficiency;
   d. increasing awareness;
   e. standardizing and automating processes;
   f. controlling, containing, and recovering from incidents;
   g. strengthening systems lifecycle security;
   h. reducing attack surfaces.

3. **Office of Management and Budget M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government[79]."** October 30, 2015. The CSIP resulted from the 30-Day Cybersecurity Sprint. The CSIP established five objectives for federal civilian agencies:

   a. "Prioritized Identification and Protection of high value information and assets;
   b. "Timely Detection of and Rapid Response to cyber incidents;
   c. "Rapid Recovery from incidents when they occur and Accelerated Adoption of lessons learned from the Sprint assessment;
   d. "Recruitment and Retention of the most highly-qualified Cybersecurity Workforce talent the Federal Government can bring to bear; and,
   e. "Efficient and Effective Acquisition and Deployment of Existing and Emerging Technology".

4. **"FACT SHEET: Cybersecurity National Action Plan[80]," February 9, 2016.** This plan initiated several actions to improve cybersecurity for the federal government, the private sector, and individuals, including the following:

[77] https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari
[78] https://obamawhitehouse.archives.gov/blog/2015/06/17/fact-sheet-enhancing-and-strengthening-federal-government-s-cybersecurity
[79] https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/CSIP
[80] https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

a. Establish the Commission on Enhancing National Cybersecurity;
b. Propose an IT modernization fund for the replacement of legacy technologies;
c. Encourage users to adopt multifactor authentication;
d. Propose a significant budget increase for federal cybersecurity efforts.

5. **"Federal Cybersecurity Research and Development Strategic Plan[81]," February 9, 2016.** The plan defined three cybersecurity R&D goals: (1) within the next 1 to 3 years, achieve the science and technology advances needed to "counter adversaries' asymmetrical advantages with effective and efficient risk management," meaning the ability to identify, assess, and respond to cybersecurity risks; (2) over the next 3 to 7 years, achieve advances to "reverse adversaries' asymmetrical advantages, through sustainably secure systems development and operation"; and (3) over the next 7 to 15 years, achieve advances "for effective and efficient deterrence of malicious cyber activities via denial of results and likely attribution."

6. **Executive Order 13718, "Commission on Enhancing National Cybersecurity [82]," February 9, 2016.** This EO established a Presidential Commission on Cybersecurity that produced the report entitled COMMISSION ON ENHANCING NATIONAL CYBERSECURITY: REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY [11], published 1st December, 2016.

7. **Presidential Policy Directive 41, "United States Cyber Incident Coordination [83]," July 26, 2016.** In 2016, President Barack Obama issued Presidential Policy Directive-41 (PPD-41), which established the procedures and standards the government must follow during cyber incidents affecting public or private sector entities. The Directive established lead federal agencies during "significant cyber incidents," or those likely to harm U.S. national security interests, foreign relations, economy, public confidence, civil liberties, public health or public safety. Additionally, the Directive requires the Departments of Justice and Homeland Security to develop and maintain a public contact list that entities can use to report incidents to government authorities.

The Directive outlined that federal government agencies were to focus on three "lines of effort" during cyber incidents: threat response, asset response and intelligence support and related activities. In case a federal agency should be the affected party, it will assume a fourth area of focus: mitigation. This effort will include controlling the effects of the cybersecurity incident on agency operations, customers and workforce. Additionally, the Directive also declared that a Cyber Unified Coordination Group was to be formed in the case of a significant cyber incident. This Group would include the lead agency for asset response, and as necessary, the following other actors: other federal agencies; representatives from state, local and tribal governments; the private sector; non-governmental organizations and international counterparts.

[81] https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf
[82] https://www.federalregister.gov/documents/2016/02/12/2016-03038/commission-on-enhancing-national-cybersecurity
[83] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

8. **The Cybersecurity Framework Implementation Guidance for Federal Agencies (DRAFT NISTIR 8170)[84]," May, 2017.** This publication assists federal agencies in strengthening their cybersecurity risk management by helping them to determine an appropriate implementation of the Framework for Improving Critical Infrastructure Cybersecurity (known as the Cybersecurity Framework). Federal agencies can use the Cybersecurity Framework to complement the existing suite of NIST security and privacy risk management standards, guidelines, and practices developed in response to the Federal Information Security Management Act, as amended (FISMA). The relationship between the Cybersecurity Framework and the National Institute of Standards and Technology (NIST) Risk Management Framework are discussed in eight use cases.

9. **Presidential Executive Order 13800 [10] on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure[85]," May 11, 2017.** EO contains three main sections devoted to the cybersecurity of federal networks, critical infrastructure and the nation. The EO calls for direct pressure on federal agency leaders; indirect pressure on industry leaders; potential increased transparency for industry cyber risk management; potential of more prominent role for Defense Department in aiding critical infrastructure with cybersecurity; increased focus on critical infrastructure at greatest risk; further focus on cyber consequence management; affirmation of importance of global cooperation; attention on cybersecurity workforce; near-term actions for public and private sector institutions, including an increased focus on the NIST Cybersecurity Framework: Implementing the NIST Framework in an enterprise-wide risk management approach -- in a way that anticipates scrutiny – as an immediate priority for federal agencies and critical infrastructure companies [12].

10. **NIST Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things[86] (IoT) (Draft NISTIR 8200), February, 2018.** Prepared by the Interagency International Cybersecurity Standardization Working Group (IICS WG), which was established in December 2015, by the National Security Council's Cyber Interagency Policy Committee (NSC Cyber IPC). Its purpose is to coordinate on major issues in international cybersecurity standardization and thereby enhance U.S. federal agency participation in international cybersecurity standardization. On April 25, 2107, the IICS WG established an Internet of Things (IoT) Task Group to determine the current state of international cybersecurity standards development for IoT. This Report is intended for use by the IICS WG member agencies to assist them in their standards planning and to help to coordinate U.S. government participation in international cybersecurity standardization for IoT. There is a strong emphasis in the report on the role of the private sector in the standardisation efforts in the US, and it states that effective U.S. government participation involves coordinating across the U.S. government and working with the U.S. private sector, as there is a much greater reliance in the U.S. on the private sector for standards development than in many other countries. Companies and industry groups, academic institutions, professional societies, consumer groups, and other interested parties are major contributors. Further, the many Standards Developing Organizations (SDOs) who provide the infrastructure for the standards development are overwhelmingly private sector organizations.

[84] https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf
[85] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
[86] https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

11. **The release of the NIST Cybersecurity Framework V1.1," April, 16, 2018.** Framework V1.1 [3] was released on April 16, 2018, following a 45-day public comment period on the second draft of Framework V1.1. This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

12. **White House eliminates cybersecurity coordinator role[87], May, 2018.** In May 2018, the Trump administration decided to eliminate the "cyber coordinator" position, the nation´s top cyber policy professional in charge of harmonizing the government´s approach to cybersecurity policy and digital warfare.

In summary, the over-riding and common themes among these cybersecurity policies in the United States include the following aspects:

- Improving the security of the nation's critical infrastructure;
- Encouraging joint efforts involving a wide variety of public- and private-sector organizations to improve global cybersecurity;
- Improving federal cybersecurity policies and practices, especially in terms of incident response capabilities;
- Using risk management principles to assess vulnerabilities and select mitigations;
- Encouraging cybersecurity information sharing among public and private-sector organizations;
- Increasing public awareness of cybersecurity;
- Increasing investments in cybersecurity research;
- Promotion of the NIST Cybersecurity Framework amongst on different stakeholders, e.g. enterprises, federal agencies, etc.;
- Not much focus on regulation as a policy solution for cybersecurity.
- Whilst focus in on "America first", within Presidential Executive Order 13800, there is an affirmation of the importance of global cooperation for cybersecurity-related challenges and solutions.

4.2 Legislation overview in the United States

4.2.1 Cybersecurity Laws in the United States

The following section contains a Cybersecurity legislative overview of the United States since 2014, as a number of legislation was enacted in relation to cybersecurity in the period starting in 2014.

1. **Public Law 113-246,** "Cybersecurity Workforce Assessment Act [88] ," December 18, 2014. This law required regular assessments of the DHS cybersecurity workforce.
2. **Public Law 113-274**, "Cybersecurity Enhancement Act of 2014 [89] ," December 18, 2014. This law encouraged the public and private sectors to work together to improve cybersecurity in terms of research and development, workforce preparedness, and public awareness.
3. **Public Law 113-282,** "National Cybersecurity Protection Act of 2014**[90],"** December 18, 2014. The purpose of this law was to codify the

[87] Source: Politico https://www.politico.com/story/2018/05/15/white-house-eliminates-cyber-adviser-post-542916
[88] https://www.gpo.gov/fdsys/pkg/PLAW-113publ246/pdf/PLAW-113publ246.pdf
[89] https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf
[90] https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf

responsibilities of the National Cybersecurity and Communications Integration Center (NCCIC).

4. **Public Law 113-283,** "Federal Information Security Modernization Act of 2014[91]," December 18, 2014. This law modified Federal Information Security Modernization Act (FISMA) to revise cybersecurity incident reporting requirements for federal agencies, clarify certain federal agency cybersecurity authorities, and streamline cybersecurity reporting.
5. **Public Law 113-291, "National Defense Authorization Act for Fiscal Year 2015[92]."** December 19, 2014. Title VIII, Subtitle D of this law contains portions of what was originally H.R. 1232, "Federal Information Technology Acquisition Reform Act" (FITARA). The law required some changes to federal information technology practices that had implications for cybersecurity, most notably "consolidation of federal data centers."
6. **Division N, Public Law 114-113,** "Cybersecurity Act of 2015[93]," December 18, 2015. The Cybersecurity Act of 2015 contains the Cybersecurity Information Sharing Act (CISA). CISA encouraged the sharing of cybersecurity threat information among public- and private-sector organizations.

4.2.2 Privacy Laws in the United States

The following section contains a Privacy legislative overview of the United States since 1974, dating back to the Privacy Act of 1974.

In the United States, there is no comprehensive federal data protection law. The closest equivalent to such a law is the Privacy Act of 1974, which is described below. Instead, the US relies on a "patchwork" of federal laws, state laws and regulations. Some of these laws apply to categories of information, such as financial or health information, while others apply to activities that rely on personal information for their execution, including telemarketing and marketing via email. These laws sometimes overlap and "contradict" one another[94]. In addition, the US systems contain guidelines and frameworks, which are self-regulatory and voluntary standards that are not enforceable by law. [95]

There are also consumer protection laws that are not privacy laws, but that also have aspects that dictate the protection and disclosure of personal data. [96]

1. Privacy Act of 1974

One of the most important hallmarks of US privacy policy, and by extension cybersecurity policy, is the Privacy Act of 1974. In essence, the law "regulates the collection, maintenance, use and dissemination of personal information by federal executive branch agencies."[97] It provides individuals with the right to request the records a federal agency has on them, the right to request a change to their

[91] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[92] https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf
[93] https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf
[94] Leuan, J. (2018). Data protection in the United States: overview. Retrieved from https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default)
[95] Leuan, J. (2018). Data protection in the United States: overview. Retrieved from https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default)
[96] Leuan, J. (2018). Data protection in the United States: overview. Retrieved from https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default)
[97] Overview of the Privacy Act of 1974 | OPCL | Department of Justice. (2015). Retrieved from https://www.justice.gov/opcl/introduction

records in the spirit of accuracy, relevance, timeliness and completeness and the right to be protected against an unwanted invasion of privacy due to the "collection, maintenance, use and disclosure of their personal information."[98] The law requires that agencies publish their system of records in the publicly accessible Federal Registrar.

2. Judicial Redress Act of 2015

The Judicial Redress Act of 2015 is directly related to the Privacy Act of 1974. It allows citizens of certain foreign countries and regional economic organizations the right to judicial redress – more specifically, the right to challenge how their data is used – under the provisions of the 1974 law. The law, which was passed in 2016, was specifically prompted by the negotiations for the US-EU Data Protection Agreement. The European Commission required the US Congress to pass a judicial redress act as part of the negotiations. US citizens in the EU had the same right before the Judicial Redress Act was passed.

3. Federal Trade Commission Act

The Federal Trade Commission Act is a federal consumer protection law that prohibits unfair or deceptive acts or practices in or affecting commerce.[99] The law gives the Federal Trade Commission (FTC) the power to seek monetary damages or other forms of "relief" for actions that have harmed consumers, emit rules that define unfair or deceptive acts and requirements to prevent such acts and investigate organizations and businesses involved in commerce, among others. The FTC has disciplined companies that fail to comply with their published privacy policies and for unauthorized disclosure of personal data.[100][101]

4. Children´s Online Privacy Protection Act (COPPA)

The US Congress approved the Children´s Online Privacy Protection Act (COPPA) in 1998. COPPA limits the collection of information from children under the age of 13 without their parents´ consent. It requires websites to post their entire privacy policy online, inform parents about their data collection policies and practices and get "verifiable consent" before collecting a child´s personal information and sharing it with third parties.[102] Under COPPA, parents have the right to review the information a website has on their child, delete their child´s information and prevent the website from collecting any further information on their child. It also requires websites to establish practices that protect the children´s information and not encourage children to engage in activities that would allow the website to collect more information than is "reasonably necessary."[103] The FTC is the primary agency in charge of enforcing COPPA.

---

[98] The Privacy Act and the Freedom of Information Act | Social Security Administration. (2018). Retrieved from https://www.ssa.gov/agency/privacyact.html

[99] Federal Trade Commission Act. (2018). Retrieved from https://www.ftc.gov/es/enforcement/statutes/federal-trade-commission-act

[100] Leuan, J. (2018). Data protection in the United States: overview. Retrieved from https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default)

[102] Protecting Children's Privacy Under COPPA: A Survey on Compliance [Ebook]. Retrieved from https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf

[103] Protecting Children's Privacy Under COPPA: A Survey on Compliance [Ebook]. Retrieved from https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf

5. Financial Services Modernization Act (Gramm-Leach-Bliley Act or GLB)

The Financial Services Modernization Act (GLB) required financial institutions to disclose their information-sharing practices to customers and allow them to declare if they want their personal information shared. This information, which includes bank balances and account numbers, is often bought and sold by banks, credit card companies and others.[104]

6. Health Insurance Portability and Accountability Act (HIPAA)

The law protects a person´s "individually identifiable health information" held by an entity. It is classified as an individual´s past, present or future physical or mental health or condition, the provision of health care provided to that individual and the past, present or future payment for the provision of health care to the individual.[105] Other common identifiers include name, address, birth date and Social Security number. Demographic data is also considered protected information. Nevertheless, HIPAA allows for the release of certain information in order to maintain high and continuous standards of care. The Department of Health and Human Services is in charge of enforcing the law.

7. Fair Credit Reporting Act

The Fair Credit Reporting Act applies to consumer reporting agencies, such as credit bureaus, medical information companies and tenant screening services. [106] Information cannot be provided to anyone who does not meet a purpose covered in the act. The law also made consumer reporting agencies responsible for investigating disputed customer information. Entities that use the information provided by these agencies and then make adverse credit, insurance or employment decisions based on said information must inform the consumers that the action has been taken due to the information provided in the reports.

8. Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)

The Controlling the Assault of Non-Solicited Pornography and Marketing Act was approved by the US Congress in 2003 and regulates commercial email. It establishes requirements that commercial messages must meet and gives users the right to have marketers stop emailing them. The messages that fall under CAN-SPAM include "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service." This also includes business to business email and messages to former customers announcing, for instance, a new product line.[107] Every email found to be in violation of the CAN-SPAM Act can face fines of up to $41,484.

9. Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) of 1986 protects "wire, oral and electronic communications while those communications are being made, are in transit, and when they are stored on computers." The law applies to emails,

[104] The Gramm-Leach-Bliley Act of 1999 (GLBA). Investopedia. Retrieved from https://www.investopedia.com/terms/g/glba.asp
[105] Summary of the HIPAA Privacy Rule. (2013). Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
[106] Fair Credit Reporting Act. (2018). Retrieved from https://www.ftc.gov/es/enforcement/statutes/fair-credit-reporting-act
[107] CAN-SPAM Act: A Compliance Guide for Business. (2009). Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

telephone conversations and electronically stored data.[108] The ECPA also safeguards the contents of files and records held by service providers.

10. Customer Online Notification for Stopping Edge-provider Network Transgressions Act (also known as the CONSENT Act)

A new bill introduced in April 2018 in the US Senate by Sens. Richard Blumenthal (D-CT) and Ed Markley (D-MA) that would require companies to obtain explicit consent from users to use, share or sell any personal information they disclose. Additionally, it would force companies to notify individuals any time data is collected, share and used and establish new security and breach reporting requirements. The CONSENT Act comes after it was revealed that consulting firm Cambridge Analytica had harvested data from up to 50 million users and used that data in targeted political campaigns. The proposed law has been referred to the Committee on Commerce, Science and Transportation in the US Senate. It would establish the Federal Trade Commission as enforcer of the new rules and would expand the commission´s power and role in online advertising.

The CONSENT Act is seen as a direct response to the EU´s General Data Protection Regulation, which went into effect in May 2018. Facebook has already said it will comply with the GDPR and announced changes to its user policies to comply with the law. One such change includes asking users whether they want Facebook to use data from its partners, e.g. websites, to show them ads. Another change will ask users if they wish to continuing sharing information that demonstrates their political views, religious views and relationship status[109].
Source: *The Verge*, 10 April 2018

4.3 U.S. Agencies Involved in Cybersecurity Policy Areas

Unlike in the EU, where the European Commission has designated specific agencies to work on its cybersecurity priorities and strategies, the United States does not have specifically designated agencies established to carry out and enforce its cybersecurity goals. The United States sets and enforces its national security policies, which include cybersecurity policy, through what is referred to as the National Security Council Interagency Process, and has designated certain entities as response agencies for cybersecurity incidents.

The following is a broad description of the process and a few of the principal agencies involved in the United States in the event of a cyber incident.

4.3.1 National Security Council Interagency Process

The National Security Council Interagency Process is the mechanism by which the president of the United States implements national security and foreign policy decisions. The process involves at least four entities: the National Security Council, the Principals Committee, the Deputies Committee and the Policy Coordination Committee[110]. The underlying rationale for the creation of this system is that one issue rarely affects only one agency, but rather influences multiple agencies. Each

[108] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22. (2013). Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285
[109] Source: *The Verge*, 10 April 2018 https://www.theverge.com/2018/4/10/17221046/facebook-data-consent-act-privacy-bill-markey-blumenthal
[110] Affairs of State: the Interagency and National Security. https://www.globalsecurity.org/military/library/report/2009/ssi_marcella.pdf

committee includes representatives from various cabinet departments, which head federal agencies on policy areas ranging from finance to defense. Additional agencies can be added as needed.

The National Security Council is the principal agency for coordinating policy related to cyber incidents. Once the policy issue has been thoroughly discussed and consensus as to next steps reached in committee, a recommendation goes to the president who makes the final decision.

4.3.2 Department of Homeland Security

PPD-41 establishes the Department of Homeland Security as the federal lead agency for asset response activities, such as providing technical assistance to affected entities, containing vulnerabilities, reducing impact of cyber incidents and identifying other affected entities, among others.

4.3.3 Office of the Director of National Intelligence

The Directive determines that the Office of the Director of National Intelligence, through its Cyber Threat Intelligence Integration Center, will be the lead agency for intelligence support and related activities. Such activities include building situational threat awareness and sharing related intelligence, integrated analysis of threat trends and events, identification of knowledge gaps and the ability to degrade or mitigate threat capabilities, among others[111].

4.3.4 Department of Justice

The Department of Justice, acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force will be the lead agency for threat response activities. These activities include carrying out law enforcement and national security investigative activities at the affected entity´s site, collecting evidence and gathering intelligence and linking related incidents, among others[112].

[111] Presidential Policy Directive – United States Cyber Incident Coordination. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[112] Presidential Policy Directive – United States Cyber Incident Coordination. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

5 STRENGTHS AND WEAKNESSES OF THE US CYBERSECURITY AND PRIVACY MARKET.

As described in section 4.1, in February, 2016, Presidential Executive Order 13718, "Commission on Enhancing National Cybersecurity[113]," established a Presidential Commission on Cybersecurity that produced a report entitled COMMISSION ON ENHANCING NATIONAL CYBERSECURITY: REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY [11], published on 1st December, 2016.

Within the remit of this report, the Commission of experts identified a number of Imperatives that needed to be addressed in order to strengthen the cybersecurity and privacy efforts in the US. Those imperatives were the following:

Imperative 1: Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks;

Imperative 2: Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy;

Imperative 3: Prepare Consumers to Thrive in a Digital Age;

Imperative 4: Build Cybersecurity Workforce Capabilities;

Imperative 5: Better Equip Government to Function Effectively and Securely in the Digital Age; and

Imperative 6: Ensure an Open, Fair, Competitive, and Secure Global Digital Economy.

As highlighted, it is interesting to note that at least two of these imperatives deal directly with actions necessary to strengthen the innovation value of cybersecurity and privacy research and development to market activities, namely numbers 2 and 6.

Each of these imperatives were described in detail and given a set of concrete actions to achieve measurable impact. This section will highlight those actions under these imperatives and try to analyse whether any of these actions have been started since the publication of the report.

For Imperative 2: Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy, the following recommendations and actions were generated by the Presidential Commission's report.

Recommendation 2.1 The federal government and private-sector partners must join forces rapidly and purposefully to improve the security of the Internet of Things (IoT).

> **Action Item 2.1.1** To facilitate the development of secure IoT devices and systems, within 60 days the President should issue an executive order directing NIST to work with industry and voluntary standards organizations to identify existing standards, best practices, and gaps for deployments ranging from critical systems to consumer/commercial uses—and to jointly and rapidly agree on a comprehensive set of risk-based security standards, developing new standards, where necessary. (SHORT TERM)
>
> **Action Item 2.1.2** Regulatory agencies should assess whether effective cybersecurity practices and technologies that are identified by the standards process in Action Item 2.1.1 are being effectively and promptly implemented

[113] https://www.federalregister.gov/documents/2016/02/12/2016-03038/commission-on-enhancing-national-cybersecurity

to improve cybersecurity and should initiate any appropriate rulemaking to address the gaps. (MEDIUM TERM)

Action Item 2.1.3 The Department of Justice should lead an interagency study with the Departments of Commerce and Homeland Security and work with the Federal Trade Commission, the Consumer Product Safety Commission, and interested private-sector parties to assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days. (SHORT TERM)

Action Item 2.1.4 The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) should develop and communicate guidelines for IoT cybersecurity and privacy best practices for rapid deployment and use. (SHORT TERM)

Analysis of what has been done vis a vis this recommendation

The action items 2.1.1 through 2.1.4 under this recommendation have largely been covered (or started) by the work of the Interagency International Cybersecurity Standardization Working Group (IICS WG), which was established in December 2015 by the National Security Council's Cyber Interagency Policy Committee (NSC Cyber IPC). Its purpose is to coordinate on major issues in international cybersecurity standardization and thereby enhance U.S. federal agency participation in international cybersecurity standardization. They are also coordinating across the US government and private sector in their activities as they recognise there is a much greater reliance in the U.S. on the private sector for standards development than in many other countries. Companies and industry groups, academic institutions, professional societies, consumer groups, and other interested parties are major contributors to their work. Further, the many Standards Developing Organizations (SDOs) who provide the infrastructure for the standards development are overwhelmingly private sector organizations. On April 25, 2107, the IICS WG established an Internet of Things (IoT) Task Group to determine the current state of international cybersecurity standards development for IoT. This resulted in a report called the *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)* [114], prepared by the Interagency International Cybersecurity Standardization Working Group. The report is intended for use by the IICS WG member agencies to assist them in their standards planning and to help to coordinate U.S. government participation in international cybersecurity standardization for IoT.

The Report's conclusions focus upon the issue of standards gaps and the effective use of existing standards. For identified priorities, the report states that agencies should work with industry to initiate new standards projects in Standards Developing Organizations (SDOs) to close such gaps. In accordance with US Government policy, it states that agencies should participate in the development of IoT cybersecurity standards and, based upon each agency's mission, agencies should cite appropriate standards in their procurements. Also, in accordance with US Government policy, agencies should work with industry to support the development of appropriate conformity assessment schemes to the requirements in such standards.

Recommendation 2.2 The federal government should make the development of usable, affordable, inherently secure, defensible, and resilient/recoverable systems its top priority for cybersecurity research and development (R&D) as a part of the overall R&D agenda.

[114] https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf

Action Item 2.2.1 The Director of the Office of Science and Technology Policy (OSTP) should lead the development of an integrated government–private-sector cybersecurity roadmap for developing usable, affordable, inherently secure, resilient/recoverable, privacy-protecting, functional, and defensible systems. This effort should be backed by a significant R&D funding increase in the President's Budget Request for agencies supporting this roadmap. (SHORT TERM)

Action Item 2.2.2 The U.S. government should support cybersecurity-focused research into traditionally underfunded areas, including human factors and usability, policy, law, metrics, and the social impacts of privacy and security technologies, as well as issues specific to small and medium-sized businesses where research can provide practical solutions. (SHORT TERM)

Analysis of what has been done vis a vis this recommendation

The National Science and Technology Council's (NSTC's[115]) Federal Cybersecurity Research and Development Strategic Plan[116] of 2016, as described in section 3.1, in its mission statement, certainly seems to address many of the items mentioned in actions 2.2.1 – 2.2.2. The strategic plan lays out a roadmap for the Near-Term Goal (1-3 years) to achieve S&T advances to counter adversaries' asymmetrical advantages with effective and efficient risk management; Mid-Term Goal (3-7 Years) to achieve S&T advances to reverse adversaries' asymmetrical advantages, through sustainably secure systems development and operation; and Long-Term Goal (7-15 years) to achieve S&T advances for effective and efficient deterrence of malicious cyber activities via denial of results and likely attribution.

In terms of US R&D and whether it is addressing these actions, the National Science Foundation (NSF) funding programme states in their synopsis[117] that "The goals of the Secure and Trustworthy Cyberspace (SaTC) program are aligned with the Federal Cybersecurity Research and Development Strategic Plan (RDSP) and the National Privacy Research Strategy (NPRS) to protect and preserve the growing social and economic benefits of cyber systems while ensuring security and privacy. The RDSP identified six areas critical to successful cybersecurity R&D: (1) scientific foundations; (2) risk management; (3) human aspects; (4) transitioning successful research into practice; (5) workforce development; and (6) enhancing the research infrastructure. The NPRS, which complements the RDSP, identifies a framework for privacy research, anchored in characterizing privacy expectations, understanding privacy violations, engineering privacy-protecting systems, and recovering from privacy violations. In alignment with the objectives in both strategic plans, the SaTC program takes an interdisciplinary, comprehensive and holistic approach to cybersecurity research, development, and education, and encourages the transition of promising research ideas into practice." Source: https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709&org=CISE&from=home. Section 2 of this deliverable outlines the types of R&D being funded by NSF in relation to these areas of importance to the national strategy. However, it was difficult to find any particular activity in relation to critical area (4), transitioning successful research into practice. It is unclear whether there is no particular funding mechanism for this kind of innovation to market activity, or whether the activities are being disseminated elsewhere.

[115] https://www.whitehouse.gov/ostp/nstc/
[116] Federal Cybersecurity Research and Development Strategic Plan https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf
[117] National Science Foundation (NSF) synopsis https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709&org=CISE&from=home

For Imperative 6: Ensure an Open, Fair, Competitive, and Secure Global Digital Economy, the following recommendations and actions were generated by the Presidential Commission's report.

Recommendation 6.1 The Administration should encourage and actively coordinate with the international community in creating and harmonizing cybersecurity policies and practices and common international agreements on cybersecurity law and global norms of behaviour.

> **Action Item 6.1.1** Within the first 180 days of the next Administration, the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices. (SHORT TERM)
>
> **Action Item 6.1.2** The Federal government should increase its engagement in the international standards arena to garner consensus from other nations and promote the use of sound, harmonized cybersecurity standards. (MEDIUM TERM)
>
> **Action Item 6.1.3** The Department of State should continue its work with like-minded nations to promote peacetime cybersecurity norms of behavior. (SHORT TERM)
>
> **Action Item 6.1.4** Congress should provide sufficient resources to the Department of Justice (DOJ) to fully staff and modernize the Mutual Legal Assistance Treaty (MLAT) process, including hiring engineers and investing in technology that enables efficiency. It should also amend U.S. law to facilitate trans-border access to electronic evidence for limited legitimate investigative purposes, and should provide resources for the development of a broader framework and standards to enable this trans-border access. (MEDIUM TERM)
>
> **Action Item 6.1.5** NIST and the Department of State should proactively seek international partners to extend the Cybersecurity Framework's approach to risk management to a broader international market. (SHORT TERM)
>
> **Action Item 6.1.6** The Department of State, DHS, and other agencies should continue to assist countries with cybersecurity capacity building in light of growing needs and recent developments. (SHORT TERM)

Analysis of what has been done vis a vis this recommendation

As described in section 4.1, The Presidential Executive Order 13800 [10] on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," of May 11, 2017, affirms the importance of global cooperation, which seems to address this recommendation straight on.

Specifically for action 6.1.1 on the appointment of an international cybersecurity ambassador, on December 27, 2016, President Trump's transition team announced that then President-elect Donald Trump intended to appoint Tom Bossert[118] to the post of Homeland Security Advisor[119] (officially titled the Assistant to the President for Homeland Security and Counterterrorism), a position that would not require Senate confirmation. Tom Bossert was officially appointed on January 20, 2017, the date of President Trump's entrance into office[120]. Tom Bossert remained in this position until April 10, 2018, and he was replaced by Robert E. Joyce, an US cybersecurity official, who served as special assistant to the President and

[118] https://en.wikipedia.org/wiki/Tom_Bossert
[119] https://en.wikipedia.org/wiki/Homeland_Security_Advisor
[120] https://en.wikipedia.org/wiki/Tom_Bossert#cite_note-appointment-4

Cybersecurity Coordinator on the National Security Council. Robert E. Joyce began serving as White House Homeland Security Adviser to President Donald Trump on an acting basis after the resignation of Tom Bossert from the position on April 10, 2018. He was in that position for just over a month until May 31, 2018. He completed his detail to the White House and returned to the National Security Agency. Within these roles as the cybersecurity coordinator, there was a number of successes, including a get tough policies on international hacking and identification of sources of ransomware attacks on the US.

In relation to international cooperation in cybersecurity standards, the NIST Framework and cooperation with like-minded countries to promote peaceful cybersecurity norms, the US has been participating in dialogues, especially the NIST framework cooperation activities in Europe. NIST have been active with the EU communities via a number of EU – US projects, including the H2020 Discovery [121], H2020 PICASSO [122], and H2020 AEGIS project [123], where they participated to a number of AEGIS round tables already to promote cooperation on the NIST) Framework for Improving Critical Infrastructure Cybersecurity.

In relation to Action Item 6.1.6, the Office of International Engagement (OIE[124]) accomplishes the homeland security mission through direct engagement with key international partners outside of the Western Hemisphere, represents DHS in U.S. and foreign fora concerning DHS international equities, and coordinates the international activities of DHS components to align them to DHS priorities. The OIE team is responsible for the overall strategic and policy relationship with foreign partners in Europe, Asia, and the Middle East, and Africa, and plays an advisory role within DHS for domestic programs with international implications. The OIE team supports senior-level engagement with counterparts throughout this Area of Responsibility and represents DHS in the U.S. interagency on matters touching DHS's priorities. In addition, there is also the International Cooperative Programs Office (ICPO [125]), which develops strong partnerships with international governments and organizations (industry and academia) to strengthen Homeland Security's knowledge of global security threats.

In summary, in terms of strengthening the cybersecurity and privacy market activities, the recommendations and actions as proposed in December, 2016, have been more or less taken into account, or started in the new President's term.

The one weakness that we can find is in the critical area of the transference of research results into innovative solutions into the marketplace. In our research carried out for section 2 of this report and for this current section, it is difficult to find any major success stories being illuminated. As previously mentioned, it may be a case that the information is either difficult to find, perhaps for commercial reasons, or the channels of dissemination aren't clearly evident to us, to readily find the information. This topic will be raised with the US members of the Cybersecurity Reflection Group established in WP1 to gather their feedback to see if they can shed some light on this particular item.

From the more industry oriented perspective, many organizations in the United States, efficiently incorporated security and privacy policies into their business processes thanks to nation-wide cybersecurity standards and best practices. Such an approach avoided burdening companies with the requirements of multiple, and often conflicting, jurisdictions. However, despite the existence of cybersecurity

[121] http://discoveryproject.eu/
[122] http://www.picasso-project.eu/project/
[123] http://aegis-project.org/
[124] https://www.dhs.gov/office-international-affairs
[125] https://www.dhs.gov/science-and-technology/st-icpo

policies, the United States' approach to cybersecurity seems to present uncertain points in some areas. Often, the industry sector is one of the most targeted in terms of cyber-attacks and public policy should be implemented accordingly. The U.S. Chamber of Commerce suggest the following recommendations[126]:

- Policymakers should discuss the United States' cyber strategy with the business community before, during, and after the strategy is written. A wide range of issues must be wrestled with among multiple government and industry parties. In the cyber arena, authorities' intentions are often not accomplished without the significant buy-in of many sectors and companies;

- The Chamber supports commerce, not conflict. Defense and resilience must be the strategy's core pillars. Indeed, a strategic priority should be to increasingly deny our opponents' ability to conduct harmful cyber activity against the business community and the nation;

- Public-private policymaking needs to spotlight increasing adherence to international norms and deterrence. The U.S. deterrence policy has so far prevented cyberattacks that may cross the line into armed conflict. But our national deterrence deficit lies in our struggle to stymie attacks by criminal groups and foreign powers that fall into the malicious middle of the attack spectrum. This middling sweep of aggressions is bookended on the one hand by relatively minor attacks (e.g., pings) and acts of war on the other.

[126] https://www.uschamber.com/2017cyberpriorities

6 CONCLUSIONS AND RECOMMENDATIONS

One of the objectives of the AEGIS project is to identify and analyse the current technological, market, policy and regulatory landscape for cybersecurity and privacy in Europe and the United States. The mapping of the cyber security landscapes is based on a common approach, which allows us to examine the similarities and differences between the cybersecurity landscape in each jurisdiction in relation to their technology, strategy, policy and innovation driven approaches in the fields of cybersecurity and privacy.

This report, "Cybersecurity and Privacy Landscape in the United States," presents the results of the analysis in 5 sections:

1. Introduction. Overall introduction to the document.
2. Cybersecurity and Privacy Technologies. This section contains a comprehensive analysis of the cybersecurity and privacy research and innovation topics in the United States, broken down within the "critical areas" as defined by the Federal Cybersecurity Research and Development Strategic Plan (RDSP [127]) [1], which has identified six areas critical to successful cybersecurity R&D: (1) Scientific Foundations; (2) Risk Management; (3) Human Aspects; (4) Transitioning successful research into practice; (5) Workforce Development; and (6) Enhancing the research infrastructure. Since we couldn't find any specific topics or ongoing projects related to critical area (4), we only analysed this to a certain degree in section 5 of the report. In addition, a sub-section on Frameworks is included in Chapter 2 to capture the substantial activity underway in the US on Frameworks for cybersecurity related subjects.
3. US Cybersecurity and Privacy Strategy, describing the current overarching strategies being undertaken in the US in relation to Cybersecurity and Privacy.
4. Policy and Legislation activities in the United States perspective for Cybersecurity and Privacy.
5. Strengths and Weaknesses of the United States Cybersecurity And Privacy Market, and ongoing activities.

From the **technological perspective**, at a high level, there is good synergy with the ongoing work in the EU, possibly with more of a focus on Critical infrastructure protection. There is a strong emphasis on standardisation, especially in key areas of interest such as the Internet of Things (IoT), cyber-physical systems (CPS), cloud computing, international promotion of the Cybersecurity Frameworks activities, and others.

From the **policy and legislative perspective**, the over-riding and common themes among cybersecurity and privacy policies in the United States include the following aspects:

- Improving the security of the nation's critical infrastructure;

[127] Federal Cybersecurity Research and Development Strategic Plan https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf

- Encouraging joint efforts involving a wide variety of public- and private-sector organizations to improve global cybersecurity;
- Improving federal cybersecurity policies and practices, especially in terms of incident response capabilities;
- Using risk management principles to assess vulnerabilities and select mitigations;
- Encouraging cybersecurity information sharing among public and private-sector organizations;
- Increasing public awareness of cybersecurity;
- Increasing investments in cybersecurity research;
- Promotion of the NIST Cybersecurity Framework amongst on different stakeholders, e.g. enterprises, federal agencies, etc.;
- Not much focus on regulation as a policy solution for cybersecurity;
- Foster multidisciplinary approach to privacy research and solutions;
- Understand and measure privacy desires and impacts;
- Develop system design methods that incorporate privacy desires, requirements, and controls;
- Increase transparency of data collection, sharing, use, and retention;
- Assure that information flows and use are consistent with privacy rules;
- Develop approaches for remediation and recovery;
- Reduce privacy risks of analytical algorithms;
- There has been swift reaction in relation to the misuse of private data, whether it was driven by the Cambridge Analytica and/or in response to the EU's GDPR.
- Whilst focus in on "America first", there is an affirmation of the importance of global cooperation for cybersecurity-related challenges and solutions.

In terms of the **market perspective**, from our analysis, the United States seems to have addressed, or started to address, a large number of concrete recommendations and actions in relation to innovation and acceleration of investment for the security and growth of digital networks and the digital economy; these were recommended by a high-level Presidential Commission appointed by President Barack Obama, and whom delivered their final report at the end of his term in December, 2016. It is refreshing to see that the recommendations and action items, in large measure, have in some way or the other, been brought forward into the new administration, and the actions are, or seem to be, in the process of being carried out.

In the last few years, business and government organizations have seen important innovation in the field of cybersecurity. In the past, policy developments were exclusively carried out by the government, but today, private organizations play a fundamental role in the protection of the networks and systems of the United States.

The United States implements a Western approach when it comes to cybersecurity policy, which looks at cybersecurity through a national security perspective Cybersecurity is now one of the main priorities within policy discussions and planning for national and global conflicts. In this context, the cyber threat presented unique concerns to the United States. To this extent, a cyber strategy

that can provide a stable and is progressively necessary, as are ways to keep critical systems protected[128].

In the light of the last updates in terms of cybersecurity policies in the United States, it is likely that there will be an immediate and rigorous review of the cyber-defense and security, and the development of cybersecurity capabilities, which will be carried out against all threats, including terrorism.

One of the most important topics of the current United States strategy is characterized by the commitment to combat cyber espionage activities. In particular, the second strategic pillar - dedicated to increasing prosperity - emphasizes the urgent need to stem the continuous illicit removal of valuable information. Therefore, in order to reduce intellectual property theft, the United States will give top priority to counterintelligence and law enforcement activities carried out by law enforcement agencies in the interest of both public and private entities.

Finally, it is evident that the cybersecurity landscape in the United States foresees a deep connection between cybersecurity and the economic prosperity of the nation. The sharing of ideas, innovations and opinions, will enable organizational and government leaders to coordinate the cybersecurity efforts and manage the challenges that could impact on the security and the resilience of the organizations.

Apart from some information found in relation to DARPA and DHS's activities, it is difficult to locate information and/or concrete results in relation to the US strategic critical area of the **transference of research results into innovative solutions into the marketplace** in the US perspective. It could simply be a case that the information is either difficult to find, perhaps for commercial reasons, and/or the channels of dissemination aren't clearly evident to us. This important topic will be raised with the US members of the Cybersecurity Reflection Group established in WP1 to gather their feedback to see if they can shed some light on this particular item.

[128] https://www.brookings.edu/blog/order-from-chaos/2017/06/14/cyber-threats-and-how-the-united-states-should-prepare/

REFERENCES

[1] Federal Cybersecurity Research and Development Strategic Plan, https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf (February, 2016)

[2] Executive Order (EO) 13636 - Improving Critical Infrastructure Cybersecurity https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[3] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 April 16, 2018, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[4] Rockefeller, J.D., et. al., Cybersecurity Enhancement Act of 2014, https://www.congress.gov/bill/113th-congress/senate-bill/1353/text (December, 2014).

[5] Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, available at

https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf (2011).

[6] National Privacy Research Strategy, (June, 2016) https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf

[7] Executive Office of the President, Big Data, seizing Opportunities, Preserving Values https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (May, 2015).

[8] Executive Office of the President, President's Council of Advisors on Science and Technology (PCAST), Big Data: A Technological Perspective, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[9] Executive Office of the President, International Strategy for Cyberspace, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. (2011)

[10] Presidential Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (2017).

[11] COMMISSION ON ENHANCING NATIONAL CYBERSECURITY: REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY, December 1, 2016, available at https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[12] Price Waterhouse Cooper (PWC), Initial takeaways from President Donald Trump's cybersecurity executive order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May, 11, 2018. Available at https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/trumps-cybersecurity-executive-order.html.

aegis

accelerating EU–US Dialogue in Cybersecurity and Privacy

Quotation:

When quoting information from this report, please use the following phrase: "Cybersecurity and Privacy Landscape in the United States. AEGIS project."

Consortium:

inmark europa

Consiglio Nazionale delle Ricerche

Waterford Institute of Technology

Hewlett Packard Enterprise

european american chamber of commerce new jersey

THE PROVIDENCE GROUP

RUTGERS

aegis-project.org

linkedin.com/company/aegis-project

@aegis_cyber