US and EU Governmental Efforts to Protect Controlled Unclassified Information from Cyber Threats

Dr. Kristina MISHEVA [a,1]
[a] *Kristina Misheva PhD, Associate Professor at the Faculty of Law, Goce Delcev University in Stip, Republic of North Macedonia*

Abstract. While the threat of cybersecurity breaches—unauthorised access to networks, applications, and data—should be a priority for businesses and organizations, it is likewise a priority for government's worldwide, and, in particular, governments are working on rules and standards intended to protect controlled unclassified information in public procurements. This is an important issue because governments share vast quantities of sensitive data with contractors through public procurements. Governments are increasingly realizing that this poses a significant risk to national security and steps should be undertaken to protect controlled unclassified information (CUI). The purpose of this article is to identify and compare those rules and standards in the United States and the European Union on the protection of controlled unclassified information and provide general recommendations. Overall, this article concludes by confirming that there are differences between the approaches taken by the US and EU to protect controlled unclassified information and that a uniform approach in the EU is recommended.

Keywords. cybersecurity, controlled unclassified information, cyber threats, public procurements, intellectual property, national security

1. Introduction

The purpose of this article is to identify and compare the rules and standards in the United States (US) and the European Union (EU) on the protection of controlled unclassified information. This is an area of concern because governments are some of the leading users of information technology in the world, and they oversee vast quantities of sensitive data which is often shared with contractors through public procurements. If this information is compromised through cyber-security breaches, it is possible that the national security of a country could be compromised. Countries have been slow to introduce measures and procedures to protect controlled unclassified information, despite the increasing number of attacks and breaches and the vast quantities of data held by individual countries and their public contractors. The EU and the US have taken vastly different approaches to this problem and there are pros and cons to each approach. Part One of this paper will explore the overall problem of the theft of intellectual property.

References

https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_3194, last visited February 2020
https://ec.europa.eu/commission/news/cybersecurity-and-free-flow-non-personal-data-eu-2017-sep-19_en
[1] Cybersecurity Maturity model certification (CMMC), Ver.1, January 2020, Introduction
[1] Source: A commissioned study conducted by Forrester Consulting on behalf of Dell: BIOS Securoty- the Next frontier for endpoint protection, April 2019, fig.1, https://www.dellemc.com/en-us/collaterals/unauth/analyst-reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf
[1] Ibid, fig.1
[1] Council of Europe, press releases, June 2017, https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[1] Kristina Misheva PhD, Associate Professor at the Faculty of Law, Goce Delcev University in Stip, Republic of North Macedonia; E-mail: kristina.miseva@ugd.edu.mk.

[1] Debora Halbert (2016) Intellectual property theft and nationalsecurity: Agendas and assumptions, The Information Society, 32:4, 256-268, DOI:10.1080/01972243.2016.1177762 online: https://www.tandfonline.com/doi/full/10.1080/01972243.2016.1177762?scroll=top&needAccess=true

[1] Ibid

[1] Ibid, pg.262-264

[1] E-COMMERCE AND CYBER CRIME: New Strategies for Managing the Risks of Exploitation; KPMG LLP, the U.S. member firm of KPMG International, 2000. .5 p.

[1] The author recognizes that government's oversee vast quantities of classified information too, which is largely governed by other processes, procedures and protocols. This paper is limited to a discussion about unclassified information.

[1] William T. Kirkwood: Protecting Controlled Unclassified Information: An Evaluation of Approaches to Protecting Sensitive Information in Public Procurement in the EU and the US, 28 P.P.L.R.,Issue4, 2019 Thomson Reuters and Contributors

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final (17 May 2016).

[1] See: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), Brussels, 22.2.2018; Directive on security of network and information systems3 (the 'NIS Directive') adopted by the European Parliament on 6 July 2016 and entered into force in August 2016, EU Directive on the combatting of fraud and counterfeiting of non-cash means of payment from April 2019, L123/18, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J.(L 119); Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), General Secretariat of the Council of the EU, June 2017,Department of Defence Directive (DoDD) 5143.01 and DoD Directive 5143.02, US.

[1] For more see the map for each country separately: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

[1] https://nvd.nist.gov/800-53

[1] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[1] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[1] CMMC, Ver.1, January 2020

[1] See Fig. 2 from CMMC, Ver.1 .4 p.

[1] Ibid . 5-6 p.

[1] William T. Kirkwood: Protecting Controlled Unclassified Information: An Evaluation of Approaches to Protecting Sensitive Information in Public Procurement in the EU and the US, 28 P.P.L.R.,Issue4 . 2019. 2 p.

[1] See more State on the Union 2017: https://ec.europa.eu/commission/news/cybersecurity-and-free-flow-non-personal-data-eu-2017-sep-19_en

[1] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), of 17 April 2019, Official Journal, L 151/15

[1] While the EU member states generally transpose most of the EU directives as soon as possible, delays are possible given the capacity and resources required to implement the directives. In some cases, it can take years before a directive is adopted and implemented by a member state, however. For example, it took almost two (2) years for the NIS directive to be transposed - vacatio legis.