Protecting Controlled Unclassified Information: An Evaluation of Approaches to Protecting Sensitive Information in Public Procurement in the EU and the US

William T. Kirkwood*

Comparative law; Cybersecurity; EU law; Public procurement; Sensitive personal data; United States

Addressing the threat of cybersecurity breaches—unauthorised access to networks, applications, data and the like—is a global priority which includes the threat to and protection of unclassified data in government systems in public procurement. This is an acutely important issue because governments are some of the leading users of information technology in the world, and they oversee vast quantities of sensitive data. The US and the EU have regulations and related standards for protecting this type of data which is known as controlled unclassified information (in the US) and sensitive non-classified information (in the EU). Despite important parallels in these efforts, there are large and potentially disruptive differences between the approaches taken by the US and the EU for protecting this information. This article will explore the various cybersecurity rules for controlled unclassified information in the EU and in the US, and will raise issues with these rules as they relate to public procurement. The article will also offer suggestions for better harmonisation between the two bodies of cybersecurity rules, so as to minimise potential trade barriers and other barriers to effective public procurement.

1. Introduction

In a recent talk, Mark Warner, the senior US Senator from Virginia, stated that the cybersecurity threat—the threat of unlawful or unauthorised access to computer systems and networks—is the number one threat to the US.[1] His warning echoed recent testimony from the Department of Defense before the House Armed Services Committee, which similarly stressed the threats that cybersecurity breaches pose to national security.[2] The European Commission has noted similar concerns for the EU.[3] It is clear that addressing cybersecurity threats is an increasingly critical priority for both the EU and the US which must be resolved with urgency.[4] To that end, legislators and standards organisations in the EU and the US are working

* William T. Kirkwood, an attorney in Washington, DC, has recently completed his Master of Laws in Government Procurement Law with highest honors at The George Washington University Law School. Any views expressed here are his alone. He would like to thank Professor Christopher R. Yukins for his assistance in preparing this work. He would also like to thank Mr Michael Bowsher, QC, Dr Luke Butler, Mr Bret S. Cohen, Mr Sandeep Kathuria and Dr Katie Smith for their generous reviews and comments on this article.

[1] Senator Mark Warner, Address at the Northern Virginia Technology Council meeting at The George Washington University (23 June 2018).

[2] Department of Defense Joint Testimony on Military Technology Transfer: Threats, Impacts, and Solutions for the Department of Defense Before the H. Armed Serv. Comm., 115th Cong. (21 June 2018) [Department of Defense Joint Testimony], available at: *https://docs.house.gov/meetings/AS/AS00/20180621/108468/HHRG-115-AS00-Wstate-BingenK-20180621.pdf* [Accessed 23 May 2019].

[3] See the European Commission's fact sheet that establishes the urgency of addressing cybersecurity due to increased cyberattacks. European Commission Press Release MEMO/17/3194, European Commission Fact Sheet, "State of the Union 2017: The Commission scales up its response to cyber-attacks" (19 September 2017), available at: *http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm* [Accessed 23 May 2019]. See also *Strengthening the EU's Cyber Defence Capabilities* (November 2018), available at: *https://www.ceps.eu/ceps-publications/strengthening-eus-cyber-defence-capabilities/* [Accessed 10 June 2019].

[4] A data breach investigations report published by Verizon identified 53,000 incidents and 2,200 confirmed data breaches in 2017. See 2018 Data Breach Investigations Report, *https://www.verizonenterprise.com/verizon-insights-lab/dbir/* [Accessed 23 May 2019]; see also "Transatlantic

individually and collaboratively to draft legislation and standards to help improve security of national computer infrastructures.[5] These efforts include working rules and standards intended to protect controlled unclassified information in government procurement, which is the focus of this article.

The US and the EU have regulations and related standards for protecting, respectively, Controlled Unclassified Information (CUI) and sensitive non-classified information. The National Institute of Standards and Technology in the US, which is part of the US Department of Commerce, has developed standards and publications intended to secure the federal government's data, including NIST SP 800-171, NIST SP 800-53, FIPS 199 and FIPS 200. The EU has developed similar standards under various regulations, directives and communications, such as the Cyber Security Act, the European NIS Directive and its related Member State implementations, and the 2017 Joint Communication on Resilience, Deterrence and Defense. These standards vary, but many have been mapped—a technical matching of protocols—to each other, so that those conforming to a standard on one side of the Atlantic can assess whether they meet a standard from the other side.[6] In a similar manner, the European Agency for Network and Information Security (ENISA) which is tasked with harmonising standards throughout the EU has mapped European security standards for sensitive non-classified information in its Technical Guidelines for the implementation of minimum security measures for Digital Service Providers to various others.[7] Yet despite this mapping, there are large differences between the approaches taken by the US and the EU for protecting this information. For example, while the US has created a set of rules that are specifically for protecting controlled unclassified information in federal procurement, the EU's approach to protecting this type of information appears to be broadly applicable to specific service providers and digital platforms and does not specifically focus on public procurement.

Moreover, alignment between these two regulatory regimes and their related standards may diverge further in public procurement, as the US is presently considering elevating the importance of cybersecurity[8] in public procurement which suggests treatment of contractors' cybersecurity measures not as mere minimum standards, but rather as a "4th Pillar" for award evaluations alongside evaluation measures related to cost, schedule and performance.[9] As a result, reasonable questions have arisen as to how government authorities from the US and the EU will move forward and effectively collaborate in combatting the threat to controlled unclassified information in public procurement. There are also serious questions as to how these authorities will make it easier and more efficient for contractors to understand and implement protective measures for controlled unclassified information in public procurement, including how public

Cybersecurity, Forging a United Response to Universal Threats", US Chamber of Commerce (2017), which advocates for a common response to the global cybersecurity threat due to the growing threat to government, individuals, and businesses, available at: *https://www.uschamber.com /TransatlanticCybersecurityReport* [Accessed 23 May 2019]. This article's focus is on cybersecurity efforts in the EU and the US because transatlantic cooperation on cybersecurity is already underway and can readily be improved; governments the world over, however, face the types of cybersecurity threats discussed here.

[5] See, e.g. Cybersecurity and Infrastructure Security Agency Act of 2017, H.R.3359, 115th Cong. (2017), to authorise the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security; this bill passed the House of Representatives but was not taken up in the Senate in the last congressional session. The National Conference of State Legislatures (NCSL) also reports that in 2018 alone, at least 36 states, together with the District of Columbia and Puerto Rico, introduced and/or considered more than 265 bills or resolutions related to cybersecurity. The NCSL reports that some of the key areas of legislative activity include improving government security practices, providing funding for cybersecurity programmes and initiatives, restricting public disclosure of sensitive security information, and promoting workforce, training, economic development. Moreover, the NCSL reports that by September 2018, at least 14 states had enacted 31 bills related to cybersecurity. See *Cybersecurity Legislation 2018*, National Conference of State Legislatures, *http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation -2018.aspx* [Accessed 23 May 2019]. See also *Strengthening the EU's Cyber Defence Capabilities* (November 2018) (fn.3 above).

[6] For example, Appendix D of NIST Special Publication 800-171 has mapped security requirements from the Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework), to controls listed in NIST SP 800-53 and to standards found in ISO 27001.

[7] Including those of the NIST Framework and ISO 27001.

[8] Department of Defense Joint Testimony on Military Technology Transfer: Threats, Impacts, and Solutions for the Department of Defense Before the H. Armed Serv. Comm., 115th Cong. (21 June 2018) [Department of Defense Joint Testimony], available at: *https://docs.house.gov/meetings/AS /AS00/20180621/108468/HHRG-115-AS00-Wstate-BingenK-20180621.pdf* [Accessed 23 May 2019].

[9] Chris Nissen, John Gronager, PhD, Robert Metzger, JD, Harvey Rishikof, JD, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War* (The MITRE Corporation, August 2018), available at: *https://www.mitre.org/sites/default /files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf* [Accessed 23 May 2019]; see below for a discussion of the 4th Pillar approach.

authorities will streamline and measure efforts by private firms to meet cybersecurity threats. This is a critical issue for both contractors and subcontractors engaged in public procurement on a global basis, where issues related to fair competition for solicitations and bid protests, compliance and reporting, and potential fraud liability, all may arise from conflicting and misunderstood requirements. In order to appreciate these and other differences in the approach taken by the EU and the US, an overview of definitions and environments is necessary.

Controlled unclassified information (CUI), which is the focus of this article, is a designation in the US for non-classified information that must be safeguarded based on applicable law, regulations, and government-wide policies.[10] In the US, CUI is defined by the US Code of Federal Regulations.[11]CUI is also defined in an agreement between the US and the EU known as the Implementing Arrangement, which addresses cooperation in the area of homeland and civil security research.[12] Although CUI is defined in the Implementing Arrangement, the term CUI is not specifically used by the EU. Rather, the most analogous term used in the EU is "sensitive non-classified information".[13] Both CUI and sensitive non-classified information are defined collectively by the Implementing Arrangement as "information or preliminary or pre-decisional data, as applicable, that is not deemed to be classified information, but to which access or distribution limitations and handling instructions have been applied in accordance with the respective laws, regulations, policies or guidelines of the Sides".[14]

The US and EU have agreed that CUI and sensitive non-classified information include personal information, but acknowledge that each are substantially broader terms that include much more than personal information.[15] Moreover, as it relates to the Implementing Arrangement, the US and the EU have also agreed to certain broad, common protocols for treating such information. For example, the US and the EU have agreed that such information should be marked, that it should not be used for purposes other than those established in the Implementing Arrangement, and that it not be released to third parties without prior consent.[16] Surprisingly, however, guidelines for handling CUI by third parties (such as the contractor community) are not set forth in the Implementing Arrangement. Rather, contractors are expected to comply with standards for protecting information from both the US and the EU. This is difficult, however, because there appear to be significant differences between the expectations of the US and the EU relating to how CUI should be handled in public procurement, in particular by the contractor community involved in proposing or delivering products and services for public procurement.

[10] Section 2(a) of Executive Order 13556 establishes CUI as information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations and Government-wide policies. See 3 C.F.R. §13556.2(a) (2010).

[11] 32 C.F.R. §2002.4(h). The Code of Federal Regulations defines CUI as "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information … or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify."

[12] Implementing Arrangement between the European Commission and the Government of the United States of America for cooperative activities in the field of homeland/civil security research, 2010 O.J. (L 125) at 54 (21 May 2010) [Implementing Arrangement]. The Implementing Arrangement was instituted in accordance with the Agreement for Scientific and Technological Cooperation between the Government of the United States of America and the European Community, signed in Washington on 5 December 1997. See Agreement for Scientific and Technological Cooperation Between the European Community and the Government of the United States of America—Intellectual Property, 1998 O.J. (L 284) at 37 (22 October 1998).

[13] Implementing Arrangement (fn.12 above), §7.1 at 56.

[14] Implementing Arrangement (fn.12 above), §§7.1, 7.3 at 56.

[15] To that end, the Implementing Arrangement establishes that "For the US, 'Controlled Unclassified Information' includes, but is not limited to, information marked 'Sensitive Security Information', 'For Official Use Only', 'Law Enforcement Sensitive Information', 'Protected Critical Infrastructure Information', 'Sensitive But Unclassified (SBU)', and may include Business Confidential Information. For the European Commission, sensitive non-classified information is information that has a marking formally approved by the European Commission's Security Directorate." See Implementing Arrangement (fn.12 above), §§7.1, 7.3 at 56. It should also be noted that the intent in the US is to protect CUI which, as indicated above, is a substantially broader term than the personal information that is addressed by the GDPR. Consequently, the approach by the US to addressing the protection of CUI that is involved in federal government procurement is likely to be more comprehensive.

[16] Implementing Arrangement (fn.12 above), §7.4 at 56.

The federal contracting community in the US has been focused in recent years on understanding and implementing requirements for protecting CUI that were established for public procurement by regulations such as DFARS 252.204-7012 (the 7012 clause), which addresses the safeguarding of covered defence information and cyber incident reporting,[17] and FAR 52.204-21, which addresses basic safeguarding of contractor information systems. Each of these public procurement regulations addresses rules for protecting CUI and requires compliance with standards developed by the National Institute of Standards and Technology (NIST), which are the primary source of cybersecurity standards in the US.[18]

In the EU, there has been quite a lot of activity focused on cybersecurity driven by, among others, the European Union Agency for Network and Information Security (ENISA),[19] Regulation (EU) No.526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No.460/2004,[20] Directive (EU) 2016/1148 regarding common levels of security of network and information systems across the Union (European NIS Directive),[21] 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 protection of personal data (the General Data Protection Regulation (GDPR)),[22] and the technical guidelines for the implementation of minimum security measures for Digital Service Providers (DSPs) (the EU Technical Guidelines).[23] While contracting authorities are free under the EU Directives to take ad hoc measures to protect information in the actual procurement process,[24] these organisations and documents are the primary sources establishing cybersecurity controls in the EU for, among other things, CUI.[25] Yet for all of this activity, there does not appear to be a specific focus in the EU on how sensitive unclassified information is to be handled in for public procurement, or by the contractor community involved with public procurement.[26] This is a significant distinction from the approach taken by the US which, as outlined above, has established regulations

[17] Covered defense information (CDI) is defined by the 7012 Clause as "unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at *http://www.archives.gov/cui/registry/category-list.html*, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is—(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."

[18] NIST issues a variety of publications including standards, handbooks, journals, data and special publications. Two such NIST special publications are NIST SP 800-171, which addresses standards for protecting CUI in nonfederal systems and organisations, and NIST SP 800-53, which provides recommended security controls for federal information systems and organisations. Accordingly, in US federal procurement there has been no shortage of focus on cybersecurity by the Federal government, its contractor community, and the industries that support them (e.g. technology consultants, compliance experts, lawyers, and the like). See fn.78 below for examples of this focus on cybersecurity.

[19] More information is available at: *https://www.enisa.europa.eu/* [Accessed 23 May 2019].

[20] Regulation (EU) No.526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No.460/2004.

[21] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016 O.J. (L 194) (19 July 2016) [NIS Directive].

[22] 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) (4 May 2016) [GDPR].

[23] Technical guidelines for the implementation of minimum security measures for DSPs (2016) [EU Technical Guidelines], available at: *https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers* [Accessed 23 May 2019].

[24] Such measures may include provisions relating to selection and award of successful bidders, and requirements for contract performance. See, e.g. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, 2014 O.J. (L94), art.21(2) at 106 (28 March 2018) [Directive 2014/24].

[25] There are other specialised decisions, such as Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission, 2015 O.J. (L 72) at 41 (17 March 2015) which addresses security specifically for the European Commission. Such will not be reviewed in this article.

[26] The GDPR indicates that the "principles of data protection by design and by default should also be taken into consideration in the context of public tenders", GDPR, Recital (78) (fn.22 above) at 15. The EU Technical Guidelines address general procurement measures to be considered by customers purchasing from DSPs. Neither the NIS Directive nor the GDPR nor EU Technical Guidelines, however, make any substantive mention of public procurement. Similarly, the EU's public procurement directive, Directive 2014/24, does not reference cybersecurity standards for public procurement. Similarly, the EU's defence procurement directive, Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, 2009 O.J. (L 216) at 76 [Directive 2009/81], does not establish cybersecurity standards for defence procurement. To be clear, the EU Directives do contain provisions relating to the protection of both classified and sensitive information, but do not include requirements or standards related to the use of such information by contractors. This may be, in part, because the Directives are addressed to Member States and not addressed to individuals.

specifically addressing public procurement. In fact, there are many distinctions between the efforts of the EU and the US in developing and applying cybersecurity standards for public procurement. These distinctions include where standards for protecting sensitive unclassified information are established, how such standards are monitored and enforced, and how efficiently and effectively such standards can be adapted to protect against evolving threats.

This article will explore these tensions and similarities between the systems for protecting sensitive unclassified information. Part 2 will review the present EU legal framework and how it is expected to evolve in the future. It will address how EU legislation applies to public procurement activities and will discuss key concepts related to the system as it has developed. Part 3 will review, in a similar fashion, the legal framework for protecting CUI in the US, and will provide a glimpse of possible future efforts, and key concepts, including a comparative view of legislation and standards in the EU and the US. This will be followed by Part 4, which will offer a discussion of selected concerns. The article will conclude in Part 5 with a summary of next steps that may be worthwhile for consideration by policy makers in each system.

2. European legal framework

The EU's efforts to manage security related to electronic communications date back at least to the late 20th century.[27] In 2004, however, the EU established the European Network and Information Security Agency (ENISA).[28] The purpose of establishing ENISA was to promote a focus on cybersecurity.[29] Europe's efforts to address the threat to cyber security continued more recently with its release of the EU Cyber Security Strategy in 2013.[30] The 2013 Cybersecurity Strategy established five priorities for combatting the cybersecurity threat.[31]

The driving consideration for the 2013 Cybersecurity Strategy appears to have been economic in nature, as well as to preserve societal freedoms and other norms. This consideration can be seen clearly in the introduction to the 2013 Cybersecurity Strategy.[32] As there appears to be little in the 2013 Cybersecurity Strategy addressing public procurement concerns, this may explain the difference between the EU and US approaches to safeguarding CUI or sensitive non-classified information in public procurement. Indeed,

[27] On 8 October 1997 the European Commission published a "Communication on ensuring security and trust in electronic communication—towards a European framework for digital signatures and encryption". See Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999 O.J. (L 013) at 1 (19 January 2000), art.1, which establishes that the Directive's purpose was to "facilitate the use of electronic signatures …".

[28] Regulation (EC) No.460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, 2004 O.J. (L 77) (13 March 2004) [Regulation 460/2004].

[29] See, e.g. Regulation 460/2004, art.1(1) at 7, which provides: "for the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market, a European Network and Information Security Agency is hereby established, hereinafter referred to as 'the Agency'".

[30] See Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Parl. Eur. Doc. (JOIN(2013) 1 final) (7 February 2013) [2013 Cybersecurity Strategy], *https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf* [Accessed 23 May 2019]; see also "Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses", Parl. Eur. Doc. (PE 536.470) (2015), *http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf* [Accessed 23 May 2019].

[31] See 2013 Cybersecurity Strategy (fn.30 above), §2 at 4–5, which established these priorities as: 1. achieving cyber resilience; 2. drastically reducing cybercrime; 3. developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP); 4. developing the industrial and technological resources for cybersecurity; 5. establishing a coherent international cyberspace policy for the EU and promote core EU values.

[32] See 2013 Cybersecurity Strategy (fn.30 above), §1.1 at 2–3, where the drafters state: "For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. … Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. … By completing the Digital Single Market, Europe could boost its GDP. … Unfortunately, a 2012 Eurobarometer survey showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases. … Cybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. … The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies. … The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online. … The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union … outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world."

it appears that the EU's approach to cybersecurity has been focused almost wholly on combatting the cybersecurity threat for the EU on a generalised basis.[33] There does not seem to be any specific strategy for combatting cybersecurity as it relates to public procurement activities as can be found in the US system.[34] This omission is mirrored in subsequent strategy documents, none of which specifically address public procurement, such as the European Agenda on Security (2015),[35] the Digital Single Market Strategy (2015),[36] and the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016).[37]

The history of cybersecurity legislation in the EU also supports this observation, as no EU legislation appears to specifically address cybersecurity requirements as they relate to public procurement or to contractors participating in public procurement activities.[38] Indeed, the Directive on Network and Information Security of 6 July 2016,[39] which is the first EU-wide directive relating to cybersecurity initiatives,[40] describes its subject matter and scope as relating to generalised European cybersecurity resilience.[41]

[33] Europe's approach with the GDPR was to create a set of cybersecurity requirements that all companies must comply with, for the protection of personal information. From a cybersecurity perspective, the GDPR addresses both how personal information is secured, and what the obligations are for reporting cybersecurity incidents that impact personal information to regulators and individuals. There are also penalties for noncompliance. Those in the US must comply with the GDPR when they handle personal information of European residents in the context of providing goods or services to those residents, but the US presently does not have such a comprehensive rule for protecting the security of its own residents' personal information. It may be instructive for the US to study the GDPR and whether and how such legislation could be implemented in the US. See Dr Aysem Diker Vanberg, "The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?" (2018) 21 J. Internet L. 1, 12; see also Alyssa Newcomb, *Could Europe Teach the U.S. a Lesson About Cyber Regulation?*, NBC News (22 September 2017), *https://www.nbcnews.com /tech/security/could-europe-teach-u-s-lesson-about-cyber-regulation-n803656*; but see Roslyn Layton and Julian Mclendon, "The GDPR: What It Really Does and How the U.S. Can Chart A Better Course" (2018) 19 Federalist Soc. Rev. 234, 247 (addressing reasons why the GDPR is not appropriate for the US, including the steep cost of compliance, prospective impairment of free speech rights, and potential for blocked content).

[34] See, e.g. DFARS 252.204-7012.

[35] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, the European Agenda on Security, COM(2015) 185 final (28 April 2015) [European Agenda on Security]. The European Agenda on Security was created in response to the call for a coordinated effort and response at the EU level, and accordingly sets forth how the EU can bring added value to its Member States in order to ensure security. Three priorities are outlined in the European Agenda on Security: tackling terrorism and preventing radicalization, disrupting organised crime, and fighting cybercrime. European Agenda on Security at 12–20.

[36] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final (6 May 2015) [Digital Single Market Strategy]. The Digital Single Market Strategy promotes the development of technologies and conditions for digital services so as to encourage economic growth through the growth of the digital marketplace. One part of this strategy is to "reinforce trust and security in digital services and in the handling of personal data". Digital Single Market Strategy at 12.

[37] See 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) [Strengthening Europe's Cyber Resilience]. This communication presents measures aimed at strengthening Europe's cyber resilience system and to promote an innovative and competitive cybersecurity industry in Europe. Strengthening Europe's Cyber Resilience at 13. See also EU cybersecurity initiatives working towards a more secure online environment, *http://ec.europa.eu/information_society /newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf* [Accessed 23 May 2019]. This is a factsheet which describes the European Commission efforts to address cybersecurity. Additionally, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 2013 O.J. (L218) at 8 (14 August 2013) [Directive 2013/40], which addresses criminal penalties for attacks against information systems, does not specifically address public procurement.

[38] See, e.g. Directive 2013/40, (fn.37 above) (addresses the strengthening of Member State cybercrime laws and criminal sanctions, but does not specifically address public procurement); Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (addressing sexual exploitation of children including offences committed in cyberspace); Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, 2001 O.J. (L149) (2 June 2001) (which addresses, among other things, fraud and counterfeiting involving computers).

[39] NIS Directive (fn.21 above).

[40] The European Commission's website on the Digital Single Market provides: the "NIS Directive is the first piece of EU-wide legislation on cybersecurity. The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level", *https://ec.europa.eu/digital-single-market/en/news/directive-security -network-and-information-systems-nis-directive* [Accessed 23 May 2019].

[41] See NIS Directive, art.1 (fn.21 above) at 11–12. The first two paragraphs of art.1 of the NIS Directive provide: "This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. 2. To that end, this Directive: (a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems; (b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them; (c) creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation; (d) establishes security and notification requirements for operators of essential services and for digital service providers; (e) lays down

Rather, as indicated by art.1.2(d), the European NIS Directive applies only to operators of essential services, and digital service providers. Accordingly, the European NIS Directive does not address any specific requirements relating to public procurement.[42] Similarly, the EU Technical Guidelines appear to focus solely on minimum standards for Digital Service Providers (DSPs), which may include Operators of Essential Services (OES).[43] As such, the application of principles, whether from the European NIS Directive or from the EU Technical Guidelines, do not appear to contemplate specific requirements for, or related to, public procurement. Instead, such principles will apply only to the operators or providers that are covered by the legislation and/or guidelines, which are limited to operators of essential services and to digital service providers.

It appears that the EU's present intent is that further legislation, including any relating to public procurement, is preferably to be addressed at the Member State level based on the principle of subsidiarity.[44] To this end, art.1.2(a) of the European NIS Directive establishes an obligation for Member States to "adopt a national strategy on the security of network and information systems".[45] Together, the omission of cybersecurity rules addressing sensitive non-classified information in public procurement, and the delegation of further strategy and requirements at the Member State level, may present challenges for, among other things, the EU's ability to consistently apply cybersecurity protections for sensitive non-classified information, and to adapt quickly to evolving threats affecting public procurement.

The EU's approach to addressing cybersecurity protection for sensitive non-classified information contrasts with the approach taken by the US, which has taken a much more direct approach to establishing and applying cybersecurity protections for CUI in the realm of public procurement.

3. US legal framework

The history of efforts in the US to protect information stored on computers dates back to the 1970s[46] and includes well-known legislation such as the Health Insurance Portability and Accountability Act,[47] the Gramm-Leach-Bliley Act,[48] the Homeland Security Act,[49] and the Federal Information Security Management Act (FISMA).[50] Similar to the EU, the US has developed security standards that are directed at protecting

obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems."

[42] However, while the initiative at the EU level may have been limited, Member States such as the UK have pursued consultation with certain governmental stakeholders in order to ensure that the definitions within the NIS Directive adequately cover public bodies in pursuit of their procurement functions. See, e.g. Consultation on the Security of Network and Information Systems Directive, available at: *https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive* [Accessed 23 May 2019].

[43] EU Technical Guidelines (fn.23 above) at 6.

[44] The European principle of subsidiarity addresses where legislative action by Member States is preferable to that of the EU. See, e.g. Consolidated Version of the Treaty on European Union, art.5, 2012 O.J. C 326/13. See also the EU's Eur-Lex glossary summarising the principle of subsidiarity, *https://eur-lex.europa.eu/summary/glossary/subsidiarity.html* [Accessed 23 May 2019]. The EU has historically relied on the principle of subsidiarity to push legislative responsibilities to Member States. See, e.g. 2013 Cybersecurity Strategy (fn.30 above) at 4 where the drafters acknowledge that the predominate responsibility for cybersecurity rests with Member States; see also NIS Directive, art.1(2) (fn.21 above), which establishes obligations for Member States to create national strategies for the security of network and information systems. A current proposal under consideration in the EU, the 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) COM/2017/0477 final—2017/0225 (COD) [2017 EU Cyber Proposal] acknowledges that the current fragmented approach to cybersecurity in the EU is not sufficient. This proposal would seek to given ENISA a permanent mandate, and would support a cybersecurity framework for, among others, ICT products and services at the EU level.

[45] NIS Directive, art.4 (fn.21 above) at 13.

[46] Federal Computer Systems Protection Act S.1766, 95th Congress (1977–1978); see also "Timeline: The U.S. Government and Cybersecurity", *The Washington Post* (16 May 2003), available at: *http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html* [Accessed 23 May 2019] (which provides an accessible history of cybersecurity efforts in the US through May 2003).

[47] Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. No.104-191, 110 Stat. 1938 (1996) which is a US federal law which protects healthcare information.

[48] Gramm-Leach-Bliley Act, Pub. L. No.106-102, S.900, 106th Cong. (1999), which is a federal law in the US that addresses how financial institutions treat the private information of individuals.

[49] Homeland Security Act of 2002, Pub. L. No.107-296, H.R. 5005, 107th Cong. which, in addition to creating the Department of Homeland Security in the US, also addressed cyber security in, among others, Title II.

[50] The E-Government Act of 2002, Pub. L. No.107-347, H.R. 2458, 107th Cong. established FISMA which included a framework for protecting, among others, government information.

digital service providers and essential services.[51] Nevertheless, as indicated earlier, the US has taken a different approach to protecting CUI in federal government acquisition efforts. It has done this by instituting protections for sensitive information involved in the performance of government contracts,[52] an approach which contrasts with the EU which appears to have only considered generalised protection requirements for certain industries.[53] In the US, these protections involve basic protections required of contractors and subcontractors who "may have Federal contract information residing in or transiting through its information system"[54] as well as more complex regulations and standards that define requirements for safeguarding of covered defence information (CDI) which is defined to include CUI contained in the CUI registry.[55] Measures similar to those established for the protection of covered defence information are under consideration for addressing CUI in the civilian space.[56]

The effort to protect CUI got its start in earnest with the Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information which was published in August 2009.[57] The CUI Report was produced by an interagency task force which reviewed a CUI framework which was established in 2008 "for the management of Sensitive but Unclassified ('SBU') terrorism-related information".[58] The CUI Report, while it was originally intended to improve the sharing of terrorism-related information,[59] concluded that a more comprehensive and uniform set of standards was necessary.[60]

Accordingly, the CUI Report established 40 recommendations for improving the protection of CUI. This CUI Report was followed by Executive Order 13556 which defined and addressed CUI.[61] EO 13556 was issued for the purpose of "establish[ing] an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies",[62] EO 13556 was codified at 32 C.F.R. §2002,[63] which "describes the executive branch's Controlled Unclassified Information (CUI) Program (the CUI Program) and establishes policy

[51] For example, the National Institute of Standards and Technology issued Version 1.1. of its Framework for Improving Critical Infrastructure Cybersecurity on 16 April 2018 , which addresses cybersecurity for critical infrastructure in the US. See National Institute for Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (16 April 2018).

[52] Cybersecurity rules for the US federal government apply to protected information involved directly or indirectly with the performance of government contracts. See, e.g. NIST 800-171 Rev. 1 (fn.68 below).

[53] It is interesting to note that a casual survey of a cross-section of practitioners, government contractors, educators, and students, did not indicate any particular consensus on why the US has taken such a focused approach on protecting CUI in public procurement. One response suggested that perhaps the role of CUI in creating "embedded" incumbents may be involved. Under this theory, the heart of the federal procurement market is shifting from the pursuit of applications to the processing of public data. The volume, complexity, and risks associated with the public data that is being processed today by government contractors has increased the likelihood that such contractors will become difficult to dislodge through competitive measures. Accordingly, the importance of requiring such contractors to protect this public data through regulation of CUI has therefore been elevated so as to ensure that necessary protection measures are in place for this data.

[54] DFARS 252.204-7012(a) (fn.82 below).

[55] DFARS 252.204-7012(a) (fn.82 below).

[56] See, e.g. Susan B. Cassidy, "DoD Further Clarifies Its DFARS Cybersecurity Requirements", Covington & Burling LLP (8 February 2017), *https://www.insidegovernmentcontracts.com/2017/02/dod-clarifies-dfars-cybersecurity-requirements/* [Accessed 23 May 2019].

[57] The Task Force on Controlled Unclassified Information, Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information (25 August 2009) [CUI Report], *https://www.archives.gov/files/cui/documents/2009-presidential-task-force-report-and-recommendations.pdf* [Accessed 23 May 2019]. This task force was initiated by President Obama who, in a memorandum dated 27 May 2009, directed the task force to review the CUI framework established for the management of sensitive but unclassified information related to terrorism, which was established in 2008. See also US Office of the Press Secretary, Classified Information and Controlled Unclassified Information (27 May 2009), *https://www.archives.gov/files/cui/documents/2009-WH-memo-on-classified-info-and-cui.pdf* [Accessed 23 May 2019].

[58] CUI Report (fn.57 above) at v.

[59] CUI Report (fn.57 above) at vii.

[60] See CUI Report (fn.57 above) at vii. Specifically, the task force concluded: "Although the CUI Framework is intended to improve the sharing of only terrorism-related information, the Task Force concluded that a single, standardized framework for marking, safeguarding, and disseminating all Executive Branch SBU is required to further the goals of: standardizing currently disparate terminology and procedures (represented by over 107 distinct SBU regimes); facilitating information-sharing through the promulgation of common and understandable rules for information protection and dissemination; and enhancing government transparency through policies and training that clarify the standards for protecting information within the Framework. A simple, concise, and standardized CUI Framework, with effective centralized governance and oversight has the best chance of both wide acceptance within the federal government and broad adoption throughout our State, local, tribal, and private sector partner communities. The successful expansion of the scope of the CUI Framework requires careful consideration of agency missions, requirements, and the processes by which SBU information is currently managed."

[61] Exec. Order No.13556, 3 C.F.R. 13556 (2010) (EO 13556).

[62] 3 C.F.R. 13556.2 (2010).

[63] 32 C.F.R. §2002 (2016).

for designating, handling, and decontrolling information that qualifies as CUI".[64] It also incorporated several NIST standards, including NIST 800-171 (Protecting Controlled Unclassified Information/Non-Federal Systems),[65] NIST 800-53 (Security/Privacy Controls),[66] FIPS 200 (Minimum Security Requirements),[67] FIPS 199 (Standards for Security Classifications).[68] These standards, as amended, are the key overarching regulations and standards that apply to the safeguarding of CUI within executive agencies that are in place today. For government acquisition purposes, however, the key provisions that guide contractor obligations for contractors handling CUI are FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, and DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (7012 Clause).[69] Both clauses apply to prime contractors as well as to all subcontractors at any tier.[70]

FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, is required to be included in "solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system".[71] It is considered a baseline provision, which provides a minimum level of controls. These minimum controls require the contractor to protect CUI and related systems and processes as contractually required minimum standards.[72]

These controls are required to protect covered "contractor information systems", which are defined as information systems that are "owned or operated by a contractor that processes, stores, or transmits Federal contract information".[73] By its terms, FAR 52.204-21 "does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556".[74] Accordingly, the FAR clause does not relieve the contractor from its obligations to comply with the Defense Federal Acquisition Regulation Supplement's 7012 Clause where it applies.

[64] 32 C.F.R. §2002.1(a) (2016) (establishing that "This part describes the executive branch's Controlled Unclassified Information (CUI) Program (the CUI Program) and establishes policy for designating, handling, and decontrolling information that qualifies as CUI").

[65] National Institute for Standards and Technology, Special Publication 800-171, Rev.1, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" (December 2016) [NIST SP 800-171 Rev.1].

[66] National Institute for Standards and Technology, Special Publication 800-53, Rev.4, "Security and Privacy Controls for Federal Information Systems and Organizations" (April 2013 (Updated 1/22/2015)) [NIST SP 800-53].

[67] National Institute for Standards and Technology, "Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems" (March 2006) [FIPS 200].

[68] National Institute for Standards and Technology, "Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems" (February 2004) [FIPS 199].

[69] DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, is important as it requires compliance with the 7012 Clause. Similar measures are under consideration for controlled unclassified information in the civilian sectors. See, e.g. FAR Case No.2017-016. See also Information Security Oversight Office, CUI Notice—2016-01: Implementation Guidance for Controlled Unclassified Information Program (which provides implementation guidance for the CUI program based on 32 C.F.R. Pt 2002), available at: *https://www.archives.gov/files/2016-cuio-notice-2016-01-implementation-guidance.pdf* [Accessed 23 May 2019].

[70] See, e.g. FAR 52.204-21(c) and DFARS 252.204-7012(m).

[71] FAR 4.1903.

[72] See FAR 52.204-21(b)(1). These controls: "(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute. (iii) Verify and control/limit connections to and use of external information systems. (iv) Control information posted or processed on publicly accessible information systems. (v) Identify information system users, processes acting on behalf of users, or devices. (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices. (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. (xii) Identify, report, and correct information and information system flaws in a timely manner. (xiii) Provide protection from malicious code at appropriate locations within organizational information systems. (xiv) Update malicious code protection mechanisms when new releases are available. (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed."

[73] FAR 52.2.04-21(a).

[74] FAR 52.204-21(2).

The 7012 clause was initially proposed in 2011,[75] and the final rule was published in 2013.[76] This rule was subsequently amended in 2015 and 2016[77] and has been the subject of an extraordinary amount of discussion due to the compliance requirements it has placed on government contractors.[78] Compliance with the 7012 Clause is required by another standard contractual clause, DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls (7008 Clause).[79] Both the 7008 Clause and the 7012 Clause apply more stringent controls to DOD solicitations than does FAR 52.204-21. Both clauses are to be used "in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items".[80]

In its present form, the 7012 Clause applies to Covered Contractor Information Systems which the clause defines as unclassified systems that are "owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information".[81] Covered Defense Information (CDI) is defined by the clause and is essentially CUI.[82] Thus, the 7012 clause applies generally to contracts and subcontracts with the Department of Defense that involve CDI that "resides in or transits through covered contractor information systems" and that must be protected by the application of certain mandated security and reporting requirements.[83]

The 7012 Clause broadly addresses the protective measures that are required to be taken by government contractors and subcontractors[84] when they are working with sensitive information.[85] The clause requires such contractors to provide "adequate security",[86] which is defined through a set of minimum security protections.[87] These minimum security protections are broadly divided into two categories: covered contractor information systems that are operated on behalf of the Government and those that are not.

[75] Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified DoD Information (DFARS Case 2011-D039), 76 Fed. Reg. 38089 (proposed 29 June 2011) (to be codified at 48 C.F.R. Pt 204 and 48 C.F.R. Pt 252).

[76] Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039), 78 Fed. Reg. 69273 (18 November 2013) (to be codified at 48 C.F.R. Pt 204, 48 C.F.R. Pt 212, and 48 C.F.R. Pt 252).

[77] See Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), 80 Fed. Reg. 51745 (26 August 2015), (to be codified at 48 C.F.R. 202, 48 C.F.R. 204, 48 C.F.R. 212, 48 C.F.R. 239, 48 C.F.R. 252); Part 252—Solicitation Provisions and Contract Clauses, 80 Fed. Reg. 56930 (21 September 2015) (to be codified at 48 C.F.R. Pt 252); Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), 80 Fed. Reg. 81474 (30 December 2015) (to be codified at 48 C.F.R. Pt 252); Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), 81 Fed. Reg. 73000 (21 October 2016) (to be codified at 48 C.F.R. Pt 202, 48 C.F.R. Pt 204, 48 C.F.R. Pt 212, 48 C.F.R. Pt 239, 48 C.F.R. Pt 252).

[78] See e.g. Robert S. Metzger, *Cybersecurity for Defense Manufacturing: New Threats Demand Heightened Response*, Bloomberg Government, 109 Fed. Cont. Rep. (BNA) 12 (27 March 2018); William C. Wagner, *A Guide To Complying With DOD's New Cybersecurity Rules A Guide To Complying With DOD's New Cybersecurity Rules*—Law360 (2015), *https://www.law360.com/* [Accessed 23 May 2019]; Jessica C. Abrahams and Kevin J. Lombardo, *United States: DoD Provides New Compliance Guidance For Contractors Regarding DFARS 252.204-7012* (2018), *http://www.mondaq.com/* [Accessed 23 May 2019]; Kenneth Weckstein and Pamela Reynolds, *Revised Cybersecurity Requirements Mean More Compliance Measures for Defense Contractors*, Bloomberg Government, 105 Fed. Cont. Rep. (BNA) 7 (23 February 2016).

[79] DFARS 252.204-7008.

[80] DFARS 204.7034(a).

[81] DFARS 204.204-7012(a).

[82] DFARS 252.204-7012(a). The clause defines covered defence information as "unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry … that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies" and is—(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract". The CUI Registry referenced in the DFARS 252.204-7012(a), is maintained by the National Archives and Records Administration in its role as CUI Executive Agent. In this role, NARA develops CUI rules and maintains a CUI Registry listing. The CUI Registry is a listing of "Controlled Unclassified Information (CUI) [which] requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended". See *https://www.archives.gov/cui/registry/category-list* [Accessed 23 May 2019]. The Registry was established in accordance with Executive Order 13556 and 32 C.F.R. Pt 2002. See *https://www.archives.gov/cui/about* [Accessed 23 May 2019].

[83] DFARS 204.7300(a).

[84] DFARS 252.204-7012(m).

[85] In September 2017, the Director, Defense Pricing/Defense Procurement and Acquisition Policy, in collaboration with the DoD Chief Information Officer and Deputy Assistant Secretary of Defense, Systems Engineering, developed and issued an Interim Guidance Memorandum concerning the implementation of DFARS Clause 252.204-7012. See *https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf* [Accessed 23 May 2019].

[86] DFARS 252.204-7012(b).

[87] DFARS 252.204-7012(b).

Covered contractor information systems that are operated on behalf of the government are subject to specific requirements such as DFARS requirements for cloud computing services,[88] and are subject to specific security requirements established by contract.[89] On the other hand, covered contractor information systems that are not operated on behalf of the government are subject to minimum security standards established by NIST. Specifically, such contractors and their systems that are not operated on behalf of the government are subject to standards set forth in NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations". Such standards were to be implemented "as soon as practical, but not later than December 31, 2017". In addition, the 7012 Clause obligates contractors to comply with various other requirements which include providing cyber incident reporting,[90] submission of discovered malicious software to the Department of Defense's Cyber Crime Center,[91] preservation and protection of media,[92] and to cooperate with forensic analyses,[93] and other requirements set out in the 7012 Clause.[94]

The government's direction to, and minimum standards for, government contractors that do not operate systems on behalf of the government but that nonetheless operate systems that process, store, or transmit covered defence information, is where the greatest distinction is found with the rules in the EU. This is because systems operated on behalf of the government typically have express standards that the contractor must abide by.[95] Covered contractor information systems that are not operated on behalf of the government but that exist "downstream" from the government nonetheless require minimum protections, which are established in the US for public procurement through the 7012 Clause and the NIST 800-171 guidelines that it incorporates. There is no such set of requirements for vendors serving public agencies at the EU level of legislation.

The US federal government requires contractors to protect covered contractor information that exist in or traverse nonfederal systems and organisations. These requirements are set forth in documents published by the US Department of Commerce's National Institute of Standards and Technology. Specifically, NIST 800-171 is a special publication[96] issued by the National Institute of Standards and Technology and which addresses the protection of CUI in contractor systems and organisations.[97] NIST 800-171 describes what it calls 14 families of security requirements, which include both basic and derived requirements.[98] These requirements are intended to protect the confidentiality of CUI in nonfederal systems and organisations.[99] The NIST 800-171 security requirements are tied to security and privacy controls found in NIST SP 800-53,[100] which are designed for federal information systems and organisations and based on the CUI Regulation discussed earlier.[101] These requirements relate to certain categories of federal information and information systems provided in FIPS 199[102] and provide minimum security requirements for federal information and information systems defined in FIPS 200.[103] These requirements are designed, among

[88] DFARS 252.204-7012(b)(1)(i).
[89] DFARS 252.204-7012(b)(1)(ii).
[90] DFARS 252.204-7012(c).
[91] DFARS 252.204-7012(d).
[92] DFARS 252.204-7012(e).
[93] DFARS 252.204-7012(f).
[94] See generally, DFARS 252.204-7012(a)-(m). The requirements in the US are evolving. See, e.g. memoranda from Kevin Fahey, Kim Herrington, and Ellen Lord (fn.138 below).
[95] Compare DFARS 204.252-7012(b)(1)(i) and DFARS 204.252-7012(b)(2) with DFARS 204.252-7012(b)(1)(ii).
[96] A Special Publication is one of several types of documents that NIST produces when it develops guidelines, standards, and recommendations. Another category of NIST publications used in US cybersecurity standards is Federal Information Processing Standards (FIPS). See generally *https://csrc.nist.gov/publications* [Accessed 23 May 2019].
[97] NIST SP 800-171 Rev.1 (fn.65 above).
[98] NIST SP 800-171 Rev.1 (fn.65 above) at 7.
[99] NIST SP 800-171 Rev.1 (fn.65 above) at 8.
[100] NIST SP 800-171 Rev.1 (fn.65 above) at 8. See also NIST SP 800-53 (fn.66 above).
[101] 32 C.F.R. Pt 2002.
[102] NIST SP 800-171 Rev.1, (fn.65 above) at 2 (FIPS 199 defines three categories of potential impact: low, moderate and high).
[103] NIST SP 800-171 (fn.65 above) at 6 (FIPS 200, among other things, specifies minimum security requirements for information and information systems used to support executive agencies).

other things, to help federal agencies comply with the Federal Information Security Modernization Act (FISMA) of 2014, which requires federal agencies to protect agency information.[104]

While NIST 800-171 does not specifically acknowledge European standards, the individual NIST 800-171 requirements are mapped to the relevant security controls from NIST SP 800-53, and are also tied to standards defined by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) in ISO/IEC 27001.[105] Likewise, the Technical guidelines for the implementation of minimum security measures for DSPs issued by ENISA, map its requirements back to both ISO/IEC as well as to NIST 800-53.[106]

Recently, there have been active discussions in the US relating to the current US focus on "minimum standards", and suggestions that the government should frame an incentivised push to improve security practices and systems on a continuous basis. These recommendations were generated from a "Deliver Uncompromised" initiative that the DOD announced on 21 June 2018.[107] These proposals were subsequently inventoried and discussed in a report issued by the Mitre Corporation titled "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War" (Mitre Report)[108] which proposed 15 courses of action underpinning a "holistic strategy for dealing with supply chain security" within DoD. These 15 courses of action were categorised as short-term, medium-term and long-term initiatives. Three of the report's recommendations together with Annex III to the report[109] are particularly important with regard to future US plans to address cybersecurity risks related to CUI.

First, the Mitre report recommends that cybersecurity should be a primary metric used by the government in the award of DoD contracts, and in the evaluation of contractor performance under such contracts. The report further suggests that cybersecurity be considered a "4th Pillar" (or evaluation criterion) in acquisition planning, equal in importance in DoD award criteria related to cost, schedule and performance. The suggested mechanism for elevating the importance of cybersecurity is through, among others, revisions to DoD Instruction 5000.02 and Defense Acquisition Guidance along the lines of the use of cybersecurity objectives in major defence acquisitions[110] as well as through the use of incentives.[111]

Secondly, in recognition of the speed at which the cybersecurity threat has evolved, and is evolving, the breadth of attacks on, among others, software, hardware and services, and in an acknowledgement of contribution of the human element to supply chain risk, the Mitre Report advocates a concerted effort to educate DoD programme and supply chain personnel and improve the expertise of those who oversee contractors with the end-result being a greater understanding and sense of ownership over the risk to the supply chain resulting from the cybersecurity threat.[112]

Thirdly, in a recommendation that is similar to the elevation of cybersecurity as a "4th Pillar", the Mitre Report recommends the use of contractual terms to incentivise the whole of industry to monitor and improve cybersecurity measures.[113] This effort would, it seems, go hand-in-hand with the effort by the government to elevate the importance of cybersecurity in DoD acquisitions. Contractors would be

[104] NIST SP 800-171, (fn.65 above) at iv. FISMA requires federal agencies to "identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency; or information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency".

[105] NIST 800-171, (fn.65 above) at 28.

[106] EU Technical Guidelines (fn.23 above) at 10. These ISO standards may provide a good opportunity for harmonising cybersecurity requirements for public procurement.

[107] Department of Defense Joint Testimony (fn.2 above).

[108] Chris Nissen, John Gronager, PhD, Robert Metzger, JD and Harvey Rishikof, JD, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War", The MITRE Corporation (August 2018), available at: *https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf* [Accessed 23 May 2019].

[109] Annex III: Ensure Supplier Readiness and Use Contract Terms, Mitre Report (fn.108 above) at 41.

[110] The Mitre Report (fn.108 above) at 15, 43.

[111] The Mitre Report (fn.108 above) at 15, 18, 20.

[112] The Mitre Report (fn.108 above) at 15, 24, 25.

[113] The Mitre Report (fn.108 above) at 15, 31.

incentivised through competition to provide the best security solutions possible during the acquisition stage, and would be further incentivised to maintain and improve security during the performance stages.

These recommendations from the Mitre Report reflect a desire by the US to improve the protection of CUI in public procurement by increasing the importance placed on cybersecurity in acquisition efforts and by amplifying the importance of awareness and education on the various threats faced by the government to its cybersecurity. It also demonstrates a capability that the US system has for protecting CUI that the EU does not currently possess to the same degree, namely that because of its centralised nature, the US system facilitates both a prompt and effective dialogue regarding enhancements to cybersecurity, as well as a relatively direct mechanism for pursuing any necessary changes. Indeed, the EU and US systems have many distinctions, which will be discussed next.

When comparing the US and EU systems for protecting CUI in public procurement, certain aspects of the system seem to present themselves as important differences. It may be, however, that the differences between the EU and US in addressing threats to the security of information in public procurement are rooted in one significant difference between the procurement systems themselves. Specifically, the EU procurement Directives, which guide public procurement in the EU are instruments that are directed primarily at Member States. Such Directives may impose obligations on Member States and on contracting authorities. Contracting authorities may also be given discretion to act under the Directives. This authority to act, while not predominately focused on individual contractors, may include the ability to impose measures on prime contractors and with respect to sub-contractors in a supply chain. By contrast, the federal procurement system in the US is directed predominately at contracting officers and on the supply chain. Accordingly, this distinction may go a long way towards explaining why each system has developed differently with regard to protecting CUI in public procurement.

Other distinctions between EU and US systems include the centralised versus decentralised nature of each system, how CUI measures are developed, applied and enforced for public procurement activities, the relative burden that each system places on contractors and government, and the ability of government and industry to react to new cybersecurity threats and measures. The following chart outlines these distinctions, which will then be discussed in Part 4.

Table 1— Selected comparisons of EU and US efforts to protect CUI or sensitive non-classified information in public procurement

Comparative Aspect	European Union	US Federal Government
Centralised versus Decentralised nature of the system and scope for protecting CUI	Largely Decentralised[114]	Centralised[115]
How CUI measures are developed, applied and enforced for public procurement activities	Direct and Indirect [116]	Direct[117]

[114] Requirements at the EU level apply to OES and DSP providers. See EU Technical Guidelines (fn.23 above) at 6. Member States may, supported by the principle of subsidiarity, impose more comprehensive requirements on contractors who work with certain sensitive and person information. See discussion on the principle of subsidiarity, (fn.44 above).

[115] Applies minimum standards to all entities working with CUI.

[116] Directly for GDPR, OES and DSP Platforms, otherwise through Member States; direct enforcement, e.g. art.57 and art.58 of Directive 2014/24; see also *https://www.cyberessentials.ncsc.gov.uk/* [Accessed 23 May 2019].

[117] Directly for all federal public procurement. See, e.g. DFARS 252.204-7012 and FAR 52.204-21 regarding the development and application of standards to public procurement. See, e.g. FAR Part 9.1 and FAR Part 9.4 regarding the enforcement of controls for CUI. For example, compliance with DFARS 252.204-7012 is required by DFARS 252.204-7008. Lack of compliance results in supply chain risk which may be result in poor CPARS and, depending on the nature of the compliance issue, may result in a finding of non-responsibility; see also DFARS 239.73; see also *A Guide To Understanding Federal Contracting Cybersecurity Rules*, West Briefing Papers, ISSUE 17-11, October 2017.

Comparative Aspect	European Union	US Federal Government
Burden on contractors and government, and impact on competition	Higher[118]	Lower[119]
Reaction by government and industry to new cybersecurity threats and measures.	Slower[120]	Faster[121]

4. Discussion of selected areas of comparison

It seems likely that a more centralised and focused approach to protecting sensitive non-classified information in public procurement will have many benefits to the EU. These include streamlining, simplifying and clarifying the cybersecurity measures that apply to public procurement in the EU, making it easier and more efficient for contractors and subcontractors to respond to such measures and compete, improving the EU's ability to enhance its security measures and promoting the EU's ability to effectively collaborate with the US and other allies to adapt security measures in response to evolving global threats. These, in turn, will collectively result in a significant improvement in national security for both the EU and its allies.[122]

4.1 Centralised versus decentralised approaches to protecting CUI or sensitive non-classified information in public procurement

As discussed earlier, the legislative and standards development bodies in the EU have focused on developing requirements and standards for certain general types of service providers[123] and for general classes of protected data.[124] Consequently, neither the European NIS Directive nor the GDPR specifically address private vendors' control of public, non-personal data in public procurement which, in comparison, is incorporated in the focus of cybersecurity rules in US federal public procurement.[125] Rather, EU cybersecurity legislation will only apply to public procurement in situations where the service or data addressed by the EU legislation is involved, and Member States are left with the obligation to adopt potentially inconsistent or incompatible national strategies for the security of network and information systems. The US federal government, by contrast, has taken a more direct approach in developing measures for protecting CUI involved in public procurement. Requirements for protecting CUI in public procurement

[118] Lack of focus on and/or a decentralised approach to addressing cybersecurity risks in the area of public procurement create more burden on both the government (which arguably has more burden managing ad hoc provisions for addressing cybersecurity risk than on ensuring that single centralised standards are implemented) and the supply chain (which is required to understand and implement measures associated with a vast number of disparate measures). The burden on suppliers may result in suppliers exiting from the pool of vendors that compete for public procurement. This could result in lower competition and potentially higher prices.

[119] Were the EU to institute fewer sources for cybersecurity rules related to CUI in public procurement through a centralised model for instituting such rules, vendors in the EU could experience fewer administrative burdens and cost in complying with such rules. See, e.g. European Commission Fact Sheet, State of the Union 2017: The Commission scales up its response to cyber-attacks (19 September 2017) (arguing for centralised cybersecurity certificates based, in part, on the reduction they would provide to administrative burden and costs for companies), available at: *http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm* [Accessed 23 May 2019].

[120] There will likely be a slower adoption of cybersecurity measures by government contractors as standards required by EU or Member States may not be consistent. Accordingly, it will be harder for contractors to adjust to these differing standards. Additionally, it will likely take longer for governments and contractors to respond to threats and related new security measures.

[121] Standards for handling CUI for US federal procurement are uniform across the entire US federal government. Accordingly, all contractors must be familiar with and educated on such standards. Accordingly, the time for contractors to get up to speed on changes to these standards will be faster, as they are already familiar with the baseline requirements.

[122] Improved security for the EU and improved ability to collaborate, will improve security globally. See, e.g. Arnault Barichella, "Cybersecurity in the Energy Sector: A Comparative Analysis between Europe and the United States", Études de L'Ifri, Ifri, February 2018 at 9 (discussing the improvements in security that can result from collaboration between the EU and the US in the energy sector).

[123] NIS Directive, Section 1.2(d) at 12.

[124] GDPR, art.1 at 32.

[125] Article 28 of the GDPR requires processors of personal data to take appropriate steps to protect the security of the data. Additionally, contracting authorities may list what organisational or technical measures they require to meet this requirement.

are established centrally through NIST and NARA, and then applied to public procurement through the FAR and its supplements such as the DFARS.

The EU should consider taking a more centralised and direct approach for addressing cybersecurity risk to sensitive non-classified information in public procurement. This could be done using existing organisations and legislation. ENISA could take the lead to create a set of standards for public procurement that are analogous to the NIST 800-171 standards.[126] These standards should be made broadly applicable to both Member State governmental agencies handling sensitive data and to the contractors that work with them. Directive 2014/24 could then be amended to require implementation of minimum standards by contractors participating in public procurement in the EU.[127] This will not only streamline the mechanism for protecting sensitive non-classified information in public procurement, but will result in improvements in the application of cybersecurity measures.[128] There are also reasons why this may be a difficult goal to accomplish in the EU, some of which may be due to the structural differences discussed earlier between the systems in the EU and US. Such difficulties might include the challenge of obtaining Member State agreement due to concerns related to national sovereignty; those related to the length of Directive 2014/24 which, according to some, may already be too long; questions as to whether the Directives are the proper vehicle for requiring and enforcing compliance with security and/or supply chain requirements; and more.[129] Nevertheless, centralisation for cybersecurity defence capabilities is already being discussed in the EU.[130] Accordingly, particularly in view of the escalating nature of cybersecurity threat, it may be appropriate to incorporate a discussion of centralisation as a means of addressing the cybersecurity risk to sensitive non-classified information in public procurement despite such difficulties.

4.2. Consistency in the application and enforcement of standards to solicitations and contracts

When contracting authorities in either the US or the EU determine that a solicitation or contract involves CUI or sensitive non-classified information, they should then develop the standards and terms that will apply to the solicitation or contract, in order to advise contractors of, among other things, the requirements for protecting the CUI or sensitive non-classified information. In the EU, however, there is no required mechanism for consistently establishing and ensuring that minimum standards are adhered to by contractors handling sensitive non-classified information in public procurement. Rather, all standards are developed by Member States or by the EU where the solicitation concerns essential services or digital services.[131]

[126] This would be similar to the effort that is proposal that is presently being considered by the EU for creating an EU cybersecurity certification framework for ICT products and services and considering the centralisation of rules governing European cybersecurity certification schemes allowing recognition of certificates in all Member States. See the 2017 EU Cyber Proposal (fn.44 above).

[127] While the EU Concessions, Utilities, and Defence Directives, respectively Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts, 2014 O.J. (L94) at 1 (28 March 2018), Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC, 2014 O.J. (L94) at 243 (28 March 2018), and Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC, 2009 O.J. (L216) at 76 (20 August 2009), are outside the scope of this article, for completeness, it should be mentioned that amendments to these directives might be considered as well.

[128] See, e.g., Mitre Report (fn.108 above) at 27 (arguing the benefits of centralising supply chain risk management due to the improved capability that results from centralisation). But see Ozment: Cybersecurity Can't Be Centralized, Troy K. Schneider, *Federal Computer Weekly*, 20 September 2016 (arguing that there may be a limit to how far responsibility for cybersecurity can be centralised), available at *https://fcw.com/articles/2016/09/20/ozment-cyber-central.aspx* [Accessed 23 May 2019].

[129] Each of these concerns can be addressed by examples in the existing directives that set precedent for the concerns raised. For example, an argument that developing and mandating compliance with certain standards for protecting sensitive non-classified information would violate the national sovereignty of Member States, begs an observation that many other existing provisions of Directive 2014/24 (e.g. Article 76 Principles of awarding contracts) already evidence a balancing effort within the EU between national sovereignty of Member States and the reasonable requirements of the EU. A full discussion of this, however, is beyond the scope of this article.

[130] See *Strengthening the EU's Cyber Defence Capabilities* (November 2018) (fn.3 above) at v.

[131] The 2017 EU Cyber Proposal affirms that "the landscape of cybersecurity certification of ICT products and services in the EU is quite patchy" and observes that Member States "often request" certification for ICT products and services from a Senior Officials Group on Information Systems Security, which is a collaborative group which consists of representatives from Member States but is not a formal EU-level organisation. See 2017 EU Cyber Proposal (fn.44 above) at 9.

This results in the potential for inconsistency in the application of standards in the EU, and inconsistencies in the enforcement of such standards.[132] In the US, on the other hand, where a federal solicitation or contract involves CUI, federal government contracting officials in the US must include clauses such as the 7012 Clause or FAR 52.204-21 in solicitations and contracts in order to inform contractors that such solicitations involve CUI, and what the minimum requirements for providing a minimum level of security to such contracts. These standards are then effectively enforced through the federal procurement system.[133] Accordingly, the system for protecting CUI in public procurement that has been established in the US provides a far greater level of consistency, particularly relating to the minimum standards with which contractors must comply for public procurement.[134]

One option that the EU might consider is establishing a mechanism for developing and applying minimum security standards to all government solicitations and contracts, regardless of where, or in which Member State, the requirements arise.[135] This would dramatically improve the consistency in standards that are used in the EU which would, among other things, make it easier on contractors and subcontractors. If this approach were to be combined with taking a more centralised and direct approach for addressing cybersecurity risk to sensitive non-classified information in public procurement discussed earlier, it might provide a compelling mechanism for reducing the cybersecurity threat to sensitive non-classified information in public procurement in Europe. As with taking a more centralised and direct approach for addressing cybersecurity risk to sensitive non-classified information in public procurement, there may be difficulties—perhaps even identical difficulties—associated with implementing this suggestion.[136] Likewise, the recognition that centralisation—and here, standardisation—is already being discussed in the EU,[137] may provide the impetus for implementing minimum standards for protecting sensitive non-classified information in public procurement.

4.3 Easing burden on contractors and subcontractors and the impact on competition

Contractors pursuing solicitations or performing under public procurement contracts involving sensitive non-classified information in the EU arguably have at least three sources of standards with which they must comply. The European NIS Directive will provide requirements if the contractor is delivering essential services or digital services, the GDPR will apply where the contractor is handling personal information,

[132] See, e.g. Feedback from: VDMA, relative to the European Commission's request related to the initiative *Review of ENISA Regulation and laying down a EU ICT security certification and labelling*, 3 August 2017, available at: *https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3436811_en* [Accessed 10 June 2019]. See also Thomas Boué, "Closing the Gaps in EU Cyber Security", *Computer Weekly.Com* (June 2015) (arguing that inconsistent approaches to cybersecurity throughout the EU in response to the NIS Directive are making it more difficult to harmoniSe policy and preparedness in the EU), available at: *https://www.computerweekly.com/opinion/Closing-the-gaps-in-EU-cyber-security* [Accessed 23 May 2019].

[133] In the US, the consequences for failing to meet standards can be wide-ranging, including termination for cause, potential fraud liability, and failed audits. Efforts to enhance compliance efforts are evolving quickly. For example, in January 2019, Ellen Lord, the Undersecretary of Defense for Acquisition and Sustainment, released a memorandum announcing her request that contractor compliance with the 7012 Clause be validated by the Defense Contract Management Agency (DCMA) through its review of contractor purchasing systems. Available at: *https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf* [Accessed 23 May 2019]. This memorandum follows other efforts to strengthen and enhance requirements provided by the 7012 Clause, including the following: Memorandum dated 5 February 2019 by Ellen Lord directing DCMA to modify certain contracts to achieve objectives enumerated in the memorandum related to cybersecurity compliance. Available at: *https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000261-19%20USD%20Signed%20TAB%20A.pdf* [Accessed 23 May 2019]; Memorandum issued on 17 December 2018 by Kevin Fahey, the Assistant Secretary of Defense for Acquisition addressing sample language for statements of work. Available at: *https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA003377-18%20ASD(A)%20Signed%20Memo%20w%20attach.pdf* [Accessed 23 May 2019]; Memorandum issued 6 November 2018 by Kim Herrington, the Acting Principle Director Defense Pricing and Contracting concerning guidance for assessing compliance and enhancing protections required by the 7012 Clause. Available at: *https://www.acq.osd.mil/dpap/pdi/cyber/docs/Guidance_for_Assessing_Compliance_and_Enhancing_Protections.pdf* [Accessed 23 May 2019].

[134] The system for protecting CUI in the US continues to evolve. This evolution appears to be moving towards more consistency in rules for protecting CUI, and towards greater efforts to ensure compliance with such efforts. See, e.g. FAR Case No.2017-016 (justified based on the need to avoid inconsistent agency-level action) and the memoranda discussed earlier (fn.138 above).

[135] This suggestion for apply consistent standards to solicitation would be similar to and would go hand-in-hand with the option mentioned earlier for centralising the management of standards.

[136] See the discussion of these concerns (fn.129 above).

[137] See *Strengthening the EU's Cyber Defence Capabilities* (November 2018) (fn.3 above) at vi.

and then the Member State that is issuing the solicitation may have additional requirements.[138] This creates a complex competitive and compliance burden for contractors. Conversely, contractors pursuing solicitations or delivering services under a contract with the US federal government are provided with one source of specific standards with which they must comply in order to be considered compliant with a solicitation's security provisions related to protection of CUI in public procurement. The contractor's efforts to meet the requirements of, for example, the 7012 Clause will then be evaluated consistently in accordance with US federal procurement rules in order to determine whether, and to what degree, the contractor has actually complied with the standards. As such, the US applies security standards consistently to all contractors working with public procurement and that come into contact with CUI.[139] This contrasts with the decentralised model in the EU which has a disparate set of rules that may (or may not) apply to public procurement depending on the type of service, type of data, or Member State where the solicitation arose.

The EU might want to consider the benefit of a centralised model for protecting sensitive non-classified information in public procurement to the contractor community pursuing European solicitation and contracts. In particular, small- and medium-sized enterprises (SMEs) competing for work will likely become more able to compete in multiple Member States, as the requirements imposed on the contractor community for protecting sensitive non-classified information in public procurement become more homogenous. The contractor community would not be the only beneficiary. A centralised model would reduce cost and administrative burden on EU governments and, due to the eased burden on contractors, would result in more competitors entering the market.[140] More competition would likely result in lower cost to European Governments.[141] It would also make it easier and faster for the EU to react to changes in cybersecurity threats.[142] Of key importance to the success of this effort, however, would be mandating compliance by Member States with a centralised standard for protecting sensitive non-classified information in public procurement. Such a mandate might distinguish this effort from less successful efforts to centralise and streamline certain other aspects of the public procurement system.[143]

4.4 Speed in reacting to new threats

In the event the EU wants to develop, enhance and then apply new cybersecurity regulations and standards to contractors pursuing public procurement opportunities, it must do this through changes in various different legislative vehicles. For example, to institute a change that would require enhanced security measures to apply to public procurement in the EU, legislation at the EU level may need to be revised in order to address services covered under the European NIS Directive (e.g. essential services or digital services) or data covered by the GDPR (e.g. personal data).[144] Additionally, Member States that have

[138] For example, Member States may insert certification requirements into public procurement tenders, based on input from the Senior Officials Group on Information Systems Security, a collaborative group which consists of representatives from Member States. See 2017 EU Cyber Proposal, fn.15 (fn.44 above) at 9. Moreover, Member States may have varied laws covering cybersecurity generally, and which may apply to public procurements. One example is Germany, where various rules apply such as Strafgesetzbuch [StGB] [Penal Code], 13 November 1998, Bundesgesetzblatt [BGBl.] 3799, as amended, §303b (Ger.) (for introduction of malware), or Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], 30 June 2017, Bundesgesetzblatt [BGBl.] 2097, as amended, §42 (Ger.) (for certain violations of the EU GDPR).

[139] US federal requirements may differ by agency such as between civilian and defence agencies as discussed earlier. Nevertheless, the point is that where standards have been established, such standards will apply consistently within such agencies. See e.g. (fn.69 above).

[140] Challenges in meeting disparate regulatory regimes for companies doing business globally, is well established. See, e.g. *https://www.forbes.com /sites/workday/2018/09/13/the-top-three-challenges-global-companies-face-and-how-to-solve-them/#5a7d43164eb3* [Accessed 23 May 2019]. The impact on trade and cybercrime resulting from harmonised rules for protecting controlled unclassified information is not within the scope of this article, but should be explored and quantified.

[141] See, e.g. Efficient and professional public procurement, European Commission Fact Sheet, 3 October 2017, available at: *http://europa.eu/rapid /press-release_MEMO-17-3544_en.pdf* [Accessed 23 May 2019]; see also Competition and Procurement, Key Findings, 2011, OECD (arguing that increased competition reduces various anticompetitive behaviors), available at: *http://www.oecd.org/daf/competition/sectors/48315205.pdf* [Accessed 23 May 2019].

[142] This, of course, depends on how such requirements are implemented.

[143] See, e.g. The European Single Procurement Document and eCertis effort. The use of this system was not, ultimately, mandatory for EU Member States. Accordingly, its success has met with mixed reviews.

[144] The GDPR defines Personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

implemented regulations controlling cybersecurity at the national level would need to amend such regulations, or implement new rules where none exist, in order to apply the new rules to economic operators pursuing public procurement opportunities for that Member State.[145] This would likely result in slower adoption of cybersecurity measures by the government contractor community as standards required by the EU or Member States and with which contractors must comply may not be consistent and, as a result, it will be harder for contractors to adjust to disparate standards required by the EU or Member States. For the same reason, there will likely be a slower reaction time to threats and related new security measures. In the US, on the other hand, a similar type of desired change in federal standards such as those addressed by the Mitre Report,[146] would be addressed centrally through NIST and NARA, and then applied to public procurement through the FAR and its supplements such as the DFARS. This would also be expected to improve the reaction time relating to new threats. This is because a centralised system would not be required to accomplish change through a lengthy process of separately engaging, understanding, educating and/or influencing changes in disparate Member State systems on new cybersecurity threats. Rather, the threat would be addressed at the centralised level, and compliance by Member States mandated. It is notable that this same benefit is presently being discussed as it relates to centralising EU cyber defence in other areas.[147]

As discussed earlier in this article, few will argue that the cybersecurity threat to government CUI or sensitive non-classified information, whether or not it is involved in public procurement, is not increasing. Accordingly, governments need to do all that they can in order to ensure that they can respond quickly to changes in the threat landscape. The decentralised approach taken by the EU for dealing with the cybersecurity threat, together with its lack of focus on public procurement, specifically, public data processed by private vendors, is likely to hamper the EU's ability to identify, react to, and remedy cybersecurity risks specific to public procurement and, importantly, the risk to contractor systems that are not operated on behalf of the government but nonetheless process sensitive non-classified information. The US, on the other hand, based on its centralised approach for federal procurement, is likely to have an easier time identifying, reacting to, and remedying cybersecurity risks. This is illustrated by the courses of action recommended in the Mitre Report which were provided in response to the DOD's Deliver Uncompromised initiative.[148] Ultimately, due to the centralised nature of protections that are in place to protect CUI, such recommendations and related changes can be discussed and implemented relatively quickly.

The EU may wish to consider the benefits of centralisation when developing, enhancing, and applying cybersecurity requirements, as well as reacting to new and evolving cybersecurity threats. This will have an obvious positive effect on national security of the EU and its Member States.

5. Conclusion

Adequately addressing cybersecurity concerns will undoubtedly remain a critical challenge for the US and the EU for the foreseeable future. As demonstrated in this article, the US had directly applied regulations and standards associated with protecting CUI to its contractor community through the 7012 Clause, which accordingly mandates the use by government contractors handling such information, to implement minimum standards defined by NIST in various guidance documents such as NIST 800-171, NIST 800-53, FIPS

data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". See GDPR, art.4(1) (fn.22 above) at 33.

[145] One example might be Germany. Today, Germany has established national laws such as its Federal Data Protection Act in order to address certain violations of existing cybersecurity rules. See, e.g. Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], 30 June 2017, Bundesgesetzblatt [BGBl.] 2097, as amended, §42 (Ger.) (fn.139 above), which penalises certain violations of the GDPR. If future EU-wide protections were desired at a later date, Germany would need to amend its national laws in order to address these new protections.

[146] See (fn.108 above).

[147] See *Strengthening the EU's Cyber Defence Capabilities* (November 2018), §7.1.1 (fn.3 above) at 54.

[148] See the earlier discussion of the Mitre Report, (fn.108 above) and pp.41 et seq.

199 and FIPS 200. The EU has chosen to follow a different path. Presently, the EU does not require the inclusion of minimum standards for cybersecurity in government solicitations and contracts involving sensitive non-classified information. Instead, the EU has chosen to implement rules for Operators of Essential Services and for Digital Service Providers at the EU level through the European NIS Directive, as well as rules for protecting personal information through the GDPR, but has not chosen to institute mandates at the EU level at this time for contractors handling sensitive non-classified information in public procurement. The EU has instead elected to leave such mandates to the Member States through the principle of subsidiarity.[149]

This creates many concerns for Member States, ranging from the potential for inadequate protection of sensitive non-classified information to the potential for overly burdensome and complex requirements that unnecessarily burden government and the supply chain. Moreover, the deferral of legislation to Member States creates the prospect for conflicts in regulations between Member States, together with the potential for multiple potentially conflicting security requirements in solicitations that may involve more than one Member State. The approach contrasts with the centralised and direct approach that the US has taken for federal procurement and creates a needlessly complex and potentially fractured mechanism for instituting security measure in the EU which adds cost to both government and contractors. Perhaps, most important, it has downstream effects on the ability of the system to protect European governments from cybersecurity threats involving sensitive non-classified information. The EU may want to reconsider its approach.

The EU may benefit by pursuing a centralised approach such as has been implemented by the US, and create a means for directly applying minimum security standards to all Member States through legislation at the EU level facilitated by ENISA. There are several benefits that should result from such a change. The first of these benefits would be consistency. ENISA might want to consider creating a set of standards for public procurement that are analogous to the NIST 800-171 standards. These standards would be made broadly applicable to both governmental agencies handling sensitive data and to the contractors that work with them. To that end, Directive 2014/24 might be amended to require implementation of minimum standards by contractors who are participating in public procurement activities through regulations similar to FAR 52.204-21 and the 7012 Clause. As with the US approach with the 7012 Clause, the EU would not need to address all possible cybersecurity standards but rather, as the US has done, make the minimum standards be a floor for compliance purposes. Such a change would prepare the governments of the EU and its Member States to most efficiently address cybersecurity risks to sensitive non-classified information in public procurement by simplifying the mechanism for developing, applying and enforcing sensitive non-classified information measures for public procurement. Such a change would also reduce the burden on contractors which would therefore encourage more contractors to enter the public procurement supply chain and increase competition. This, together with the reduction in burden to the government, would reduce cost to government in the EU for products and services obtained through public procurement. Finally, a centralised model would likely improve Europe's ability to respond to new cybersecurity threats and to react with new security measures.

[149] See (fn.44 above).