Cybersecurity, Encryption, and Defense Industry Compliance with United States Export Regulations

Rose Richerson Eichler
rosanne.r.eichler@lmco.com

Follow this and additional works at: https://scholarship.law.tamu.edu/journal-of-property-law

Part of the President/Executive Department Commons

Recommended Citation
Available at: https://scholarship.law.tamu.edu/journal-of-property-law/vol5/iss1/2

This Symposium Article is brought to you for free and open access by Texas A&M Law Scholarship. It has been accepted for inclusion in Texas A&M Journal of Property Law by an authorized editor of Texas A&M Law Scholarship. For more information, please contact areteen@law.tamu.edu.
I. INTRODUCTION

Exports of technology and items containing technical information are regulated by the United States government. United States export control regulations exist to help protect national security, economic, and political interests. United States defense industry companies manufacture products and develop technologies and information that the United States has a particular interest in protecting. Therefore, defense industry companies must comply with United States export regulations.

† Rose Richerson Eichler is a Texas A&M University School of Law alum and former staff member of the Journal of Property Law. Mrs. Eichler is a regulatory compliance analyst for the International Trade Compliance Office, Lockheed Martin Aeronautics in Fort Worth, Texas.

2. 15 C.F.R. § 730.6 (2018).
3. See generally 22 C.F.R. § 120.
control regulations when exporting items and information to their international partners and customers. An “export” not only includes shipments of hardware or other tangible assets to foreign end-users but also includes the sharing of certain types of information with foreign recipients in the form of phone conversations, emails, meetings, conferences, presentations, and so on. Many employees of defense industry companies travel internationally with company issued laptops and cellphones containing company information that could be viewed by foreign persons. All of these activities are considered exports and may require prior authorization from the United States government under export control regulations. Failure to follow export regulations could result in a violation requiring a report to the United States government that may result in civil penalties or criminal charges. Additionally, intentional as well as unintentional releases of information to certain foreign persons could be detrimental to a defense industry company’s business and reputation and may even result in security concerns for the United States.

Although the government has an interest in regulating defense industry companies’ technology and information, critics argue that strong export control regulations may result in invasions of privacy, violations of free speech, and a displacement of the United States as a leader in a world of technological advancement. However, despite current regulations, defense industry information is still at risk of cyberattacks and inadvertent data releases, creating potential threats to national security and the security of company technology and information.

In an effort to secure company and sensitive information while exporting, defense industry companies utilize encryption and other cybersecurity measures. Advancing technologies in cybersecurity can help the government and defense industry companies by bolstering the security of their information. These same advancements can also aid attackers in breaking through cybersecurity defenses. Some advances in technology are even preventing law enforcement from gathering necessary information to conduct investigations when cyber-
attacks occur, making it difficult to identify criminal actors and seek justice.

The United States government faces challenges in creating and updating regulations to keep up with consistently advancing technology. Likewise, defense industry companies must adhere to government regulations by creating robust compliance programs, but they should also implement security and compliance measures above and beyond what the government requires to ensure more effective security for their technology and information.

This Article discusses the effect of advancing cyber technology; United States export regulations; reporting requirements related to the export of encrypted items; and encryption technology in the defense industry. First, the Article defines encryption and encrypted items. Second, the Article explains United States regulations of exports and specifically, regulations related to encryption and encrypted items. Third, the Article explains the need for defense industry companies to export and to use encrypted items. Fourth, the Article analyzes criticisms of export regulations and the differing views on United States controls. Fifth, the Article will discuss the complexities of complying with export regulations and defense industry compliance programs. Sixth, the Article examines the outlook for encryption technology, the future of regulations related to cybersecurity, and the outlook for defense industry security measures and compliance with regulations.

II. ENCRYPTION AND ENCRYPTED ITEMS

Sending information over the internet leaves it vulnerable to interceptions from other internet users while it is traveling to its intended destination. Encryption is “the ability to store and transmit information in a form that is unreadable to anyone other than intended persons.” The currently preferred method of encryption is end-to-end encryption—when only the sender and recipient of the information can decrypt the data with a special key. Only the sender and recipi-
Encryption technology got its start during World War II with mechanical machines that evolved into electronics and computers by the 1960s. Encryption is now used in standard business transactions, such as money transfers or log-in options for websites. In addition to business and industry use, individuals use encryption for the transfer of information over email. Use of encryption to protect data is increasing for businesses and individuals. Engineers often build encryption software into laptops, and owners can easily use the software. The key is setting a strong password to ensure only the user and the intended recipient can access an encrypted file.

In 1977, IBM created and the National Security Agency modified the Federal Information Processing Standard (“FIPS”) 46—which was the current Data Encryption Standard (“DES”)—and it utilized a 56-bit key ($2^{56}$ or 72,057,594,037,927,936). The National Institute of Standards and Technology determines these standardizations although it is a non-regulatory federal agency. As technology advanced, DES was breakable by the 1990s, and two Belgian developers created its replacement in 2000. By November 2001, FIPS 197 was published for the standard encryption used today: Advanced Encryption Standard (“AES”) which requires both senders and receivers to use the same key to decipher the encrypted code. AES requires users to securely store their key, so it is not acquired by unintended users.
128-, 192-, and 256-bit keys, making cyberattacks more difficult than DES.\textsuperscript{22} The current standard AES is FIPS 140-2.\textsuperscript{23}

Encryption is used in defense industry production, manufacture, and company assets provided to all employees, such as company-issued laptops and cellphones. The use of encryption assists companies in safeguarding their products, and encryption should be utilized to protect the nation's technology and information produced within the defense industry. Defense industry companies should consider technology standards when choosing encryption products and services, and the companies must also comply with United States government export regulations when exporting encrypted items and information.

\section*{III. Export Regulations}

The International Traffic in Arms Regulations ("ITAR") and the Export Administration Regulations ("EAR") are the two primary regulations that defense industry companies are required to comply with when exporting their products and information to foreign recipients.\textsuperscript{24} The Department of State implements the ITAR and the ITAR controls all items listed on the United States Munitions List ("USML").\textsuperscript{25} The Department of Commerce implements the EAR and the EAR controls all items found on the Commerce Control List ("CCL").\textsuperscript{26} The USML contains defense articles, defense services, and technical data related to defense articles.\textsuperscript{27} The CCL contains "dual-use" items, or items that can be used for a civil or military purpose.\textsuperscript{28}

For the export of items on the USML, the ITAR requires an export authorization prior to export.\textsuperscript{29} Applications for export authorizations must be submitted to and approved by the Department of State, Office of Defense Trade Controls before a company may export USML items.\textsuperscript{30} Some items on the USML may qualify for an exemption, in which case prior approval for export is not required, though there are other requirements and limitations to using an exemption.\textsuperscript{31} For the export of items on the CCL and any other items not listed on the USML, the EAR may require an export authorization prior to export.

\begin{itemize}
\item \textsuperscript{22} \textit{Id.}
\item \textsuperscript{24} 22 C.F.R. §§ 120-130 (2017); 15 C.F.R. §§ 730–774 (2018).
\item \textsuperscript{25} 22 C.F.R. §§ 120.1–2.
\item \textsuperscript{26} 15 C.F.R. §§ 730.1, 738.1(a)(1).
\item \textsuperscript{27} 22 C.F.R. §§ 120.2, 120.4.
\item \textsuperscript{28} 15 C.F.R. § 730.3.
\item \textsuperscript{29} 22 C.F.R. §§ 123.1, 124.1.
\item \textsuperscript{30} \textit{Id.}
\item \textsuperscript{31} 22 C.F.R. § 123.16.
\end{itemize}
though many items will qualify for an exception or may not require an export authorization at all.  

Failure to comply with the ITAR or EAR constitutes a violation that could result in monetary penalties, criminal charges, or other penalties for companies and individuals. However, both the Department of State and the Department of Commerce allow companies to submit reports disclosing discovered violations. The submission of a disclosure could decrease or eliminate any penalties though the decision is at the discretion of the regulating agency. A violation could be any of the following: (1) exporting without an approved export authorization when one is required; (2) failing to comply with the requirements of an approved export authorization; and (3) submitting false or misleading annual or semiannual reports, etc.

The shipment of manufactured products overseas is only a portion of international defense industry transfers that require compliance with export control regulations. Defense industry companies also discuss technical information with foreign persons over the phone, in meetings, through email, and during presentations, and thus, these international transfers are exports that may be controlled by export control regulations.

A. Exports

The Merriam-Webster defines the word “export” as “to carry away” or “to carry or send (something, such as a commodity) to some other place (such as another country).” Dictionary.com defines “export” as “to ship (commodities) to other countries or places for sale, exchange, etc.” and “to send or transmit (ideas, institutions, etc.) to another place, especially another country.”

Those who do not regularly ship items internationally may consider an export to be the shipping of a tangible item to an international destination. They may even consider an “export” to be a more official transaction that involves special shipping paperwork and government oversight. That idea is partially correct, but within the defense industry and for United States government agencies, such as the Depart-

32. 15 C.F.R. § 730.7 (“A relatively small percentage of exports and reexports subject to the EAR require an application to BIS for a license. Many items are not on the Commerce Control List (CCL) (Supplement No. 1 to §774.1 of the EAR), or, if on the CCL, require a license to only a limited number of countries. Other transactions may be covered by one or more of the License Exceptions in the EAR. In such cases, no application need be made to BIS.”).


34. 22 C.F.R. § 127.12; 15 C.F.R. § 764.5.

35. 22 C.F.R. § 127.12; 15 C.F.R. § 764.5.

36. 22 C.F.R. § 127.1; 15 C.F.R. § 764.2.


Compliance with U.S. Export Regulations

2019

Compliance with U.S. Export Regulations

The Department of State and the Department of Commerce, an “export” can include more than just the shipping of tangible materials abroad. The EAR explains:

Certain actions that you might not regard as an “export” in other contexts do constitute an export subject to the EAR. The release of technology to a foreign national in the United States through such means as demonstration or oral briefing is deemed an export. Other examples of exports under the EAR include the return of foreign equipment to its country of origin after repair in the United States, shipments from a [United States] foreign trade zone, and the electronic transmission of non-public data that will be received abroad.\(^39\)

For international companies in the defense industry, the ITAR and EAR define “export.” The ITAR defines an export as “[a]n actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner,”\(^40\) but also includes the transfer of technical data to a foreign person whether that foreign person is located in the United States or outside of the United States, otherwise known as a “deemed export.”\(^41\) As the ITAR is specific to regulation of defense articles, an export can also include the transfer of ownership, control, or registration of an aircraft or any other item subject to the ITAR by a United States person to a foreign person, including an embassy or any of its agencies located in the United States.\(^42\) The ITAR also recognizes the performance of defense services for a foreign person as an export, whether or not that service occurs abroad or in the United States.\(^43\) A defense service can include providing assistance, such as training, in the “design[ing], develop[ing], engineering, [and] manufactur[ing],” etc. of a defense article, providing a foreign person with technical data as defined by the ITAR or military training of foreign forces.\(^44\)

Under the ITAR and EAR a “foreign person” is someone who is not a citizen or permanent resident of the United States, a company incorporated in another country, or a foreign government.\(^45\) Under the ITAR specifically, if someone (or a company) releases technical data to a foreign person who holds citizenship in multiple non-United States countries, the United States considers that release an export to each country where the foreign person holds citizenship.\(^46\)

The ITAR controls the export of “technical data,” which is any information “required for the design, development, production, manu-

---

39. 15 C.F.R. § 730.5(c).
40. 22 C.F.R. § 120.17(a)(1).
41. Id.
42. Id. §§ 120.17(a)(3)–(4).
43. Id. § 120.17(a)(5).
44. Id. § 120.9(a)(1)–(3).
45. Id. § 120.16; 15 C.F.R. § 772.
46. 22 C.F.R. § 120.17(b).
facture, assembly, operation, repair, testing, maintenance or modification of defense articles." Technical data "includes information in the form of blueprints, drawings, photographs, plans, instruction or documentation." Technical data does not include any information officially released to the public, basic marketing information, or information that can be taught in engineering courses.

Similarly, the EAR controls the export of "technology" which is "information necessary for the ‘development,’ ‘production,’ ‘use,’ operation, installation, maintenance, repair, overhaul, or refurbishing” of an item not listed on the USML. The defense industry commonly refers to ITAR technical data and EAR technology as "export controlled information.”

Therefore, the ITAR and EAR restrict the movement of any item found on the USML and CCL whether tangible or intangible. This interchange includes the shipment of defense articles, commercial hardware, tools, equipment, or other produced or manufactured items from the United States to a foreign country. An export could also occur in a number of other ways that may not seem apparent when first reading the regulations.

For example, an email sent to a foreign person with an attached document that contains ITAR technical data is considered an export and would require an export authorization prior to sending. A telephone conversation between United States citizens and citizens of France detailing EAR technology may require a Department of Commerce export license prior to conducting the call. A defense industry company employee traveling for business and using his company laptop to view ITAR technical data may inadvertently cause an export if a citizen of the United Kingdom glances at the employee’s laptop screen.

It becomes easy to see from the above examples how critical it remains for defense industry companies to understand export regulations. The risks are even higher for companies exporting sensitive or classified information, and companies should take appropriate security measures to protect the information. Encryption is one method that defense industry companies can use to protect their information.

B. Encryption Regulations

The Department of State previously regulated encryption exports, which were listed on the USML because, due to their advanced technological capabilities compared to what the rest of the world was producing at the time, they were viewed and therefore classified as

---

47. Id. § 120.10(a)(1)
48. Id.
49. Id. § 120.10(b).
50. 15 C.F.R. § 772.
munitions. In 1996, President Clinton’s Executive Order 13026 transitioned encryption software from the USML to the CCL and altered regulation from the Department of State to the Department of Commerce. At that time, the Bureau of Export Administration (BXA) was the governing jurisdiction; in 2002, BXA became the Bureau of Industry and Security (BIS).

The Clinton Administration is responsible for enacting new measures to reform encryption export regulations. For example, the administration instituted policy that permitted more powerful encryption technology and enabled the mass marketing of higher strength encryption products.

Some encrypted items require an export license issued by the BIS before a company may export the encrypted items to a foreign recipient. However, many encrypted items qualify for the Encryption Commodities, Software and Technology (“ENC”) exception under the EAR and do not require a license for export, but requirements and limitations exist when using the ENC exception. For example, the exporter must list the exception on all shipping documents, and some exports may need to be reported to BIS annually or semiannually. Exporters may use the ENC exceptions for most encrypted items, but some items destined for certain locations may require a license before export.

The EAR contains multilateral controls and unilateral controls for the export of encrypted items. Member nations to the Wassenaar Arrangement determine multilateral controls, and the United States government determines unilateral controls.

Companies exporting encrypted items have three separate reports to submit to BIS: (1) EAR § 740.17(e)(1) requires semiannual reporting of all exports of encrypted items to all foreign destinations except Canada, although some items may be excluded from the report, such as items with a key length that is less than 64 bits; (2) EAR § 743.1 Wassenaar Arrangement; and (3) § 742 Supplement 8: Self-Classifica-

54. Pasko, supra note 8, at 341.
55. Id.
56. Bureau of Indus. and Sec., supra note 54.
58. Id. §§ 762.2, 743, 764.4.
60. Bureau of Indus. and Sec., supra note 54.
61. 15 C.F.R. § 740.17(e)(1).
tion Report for Encryption requires companies to annually report on certain encryption items that the company exported or re-exported.\textsuperscript{62}

Although it may be cumbersome for defense industry companies to track, record, and report on the export of encrypted items and encryption technology, the United States government has a valid interest in regulating these transactions.

\textbf{C. Government Interest in Regulating Exports}

To promote world peace and ensure security and further foreign policy in the United States, the President shall control the import and export of defense articles and services by providing guidance to United States persons who export and import defense articles and services.\textsuperscript{63} The President shall determine what items constitute defense articles and defense services, and the list of these items is the USML. The President promulgates the ITAR.\textsuperscript{64}

General EAR provisions “are intended to serve the national security, foreign policy, nonproliferation of weapons of mass destruction, and other interests of the United States, which in many cases are reflected in international obligations or arrangements.”\textsuperscript{65} Encryption is a dual-use item because it can be used for commercial purposes or for military purposes.\textsuperscript{66} The United States government is interested in controlling the export of encryption and encrypted items because of the effects these exports have on the United States economy and law enforcement.\textsuperscript{67}

Regulating the export of the United States’ produced and developed encrypted items and information requires the government’s understanding of cybersecurity services and risks.

\textbf{D. Government Interest in Cybersecurity}

The United States government takes additional measures to ensure national cybersecurity in addition to export regulations. The United States Cyber Command was established in October 2010 and:

Plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed,

\begin{itemize}
\item \textsuperscript{62} See Innokent Pyetranker, \textit{An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement}, 13 NW. J. TECH & INTELL. PROP. 153, 164 (2015) (“[C]oncerted action—rather than passive pessimism—must be our response to cyber threats . . . Encryption technology is dual-use in that it can be used to, for instance, protect consumer data (a civilian purpose) and intercept enemy communications during armed conflict and prevent terrorist attacks (military purposes.”).
\item \textsuperscript{66} 22 U.S.C.A. § 2778 (2014).
\item \textsuperscript{64} 15 C.F.R. § 730.6.
\item \textsuperscript{65} Id. at 165.
\end{itemize}
conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace, and deny the same to our adversaries. The Command unifies the direction of cyberspace operations, strengthens DoD cyberspace capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM is designing the cyber force structure, training requirements and certification standards that will enable the Services to build the cyber force required to execute our assigned missions. The command also works closely with inter-agency and international partners in executing these critical missions.\footnote{68}

A new policy bill pushing for better cybersecurity measures for the Department of Defense is currently supported by some United States senators.\footnote{69} One portion of this proposed bill is to give the Secretary of Defense more authority in utilizing cyber activities to conduct military operations.\footnote{70} This move by senators comes after “recent developments with DoD’s primary warfighting organization, United States Cyber Command, and its new status as a fully unified command.”\footnote{71} Additionally, “the Senate panel suggested giving the executive branch the authority to direct Cyber Command to ‘take appropriate and proportional action through cyberspace to disrupt, defeat, and deter systematic and ongoing attacks by Russia in cyberspace.’”\footnote{72}

The United States is not the only country concerned with cybersecurity and the regulation of exports and imports. Other countries conduct business internationally and recognize the need for standardized practices and oversight of international exchanges of information and technology.

E. International Regulations

In addition to United States export regulations, other countries maintain their own export control regulations. Defense industry companies involved in exporting and importing goods need to familiarize themselves with other countries’ export control laws to ensure compliance. Many countries agree that cyberattacks pose a significant threat to international business, and efforts to protect against such threats

\footnote{70. Id.}
\footnote{71. Id.}
\footnote{72. Id.}
are discussed and implemented by these concerned parties who hope to harmonize export standards.\textsuperscript{73}

By combining efforts and creating a harmonized system of export controls, countries may be able to work together in successfully preventing cyberattacks and data hacking initiated by their shared enemies.\textsuperscript{74} In creating a common encryption export control regime, the United States can replace extreme regulations and avoid the risk of losing market share to competing countries with lesser controls.\textsuperscript{75} Additionally, these combined efforts "will strengthen the United States' encryption industry and in doing so, further American security interests."\textsuperscript{76}

During the Cold War, Soviet powers acquired western technology, and as a result of fear that this technology would be used against the West, the Western Bloc powers created the Coordinating Committee for the Control of Multinational Trade ("COCOM").\textsuperscript{77} In 1996, after the Cold War, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (The Wassenaar Arrangement) replaced COCOM.\textsuperscript{78} Thirty-three member states met to add items to the Munitions List and the List of Dual-Use Goods and Technologies that are subject to control under the Wassenaar Arrangement.\textsuperscript{79} The goal of the Wassenaar Arrangement is to coordinate with member states to create an export control system for all parties.\textsuperscript{80} Each member state commits to controlling these lists, controlling the movement of items on the lists, and to sharing information with each other.\textsuperscript{81} In 1996, more member states joined after the initial meeting, and more could still join should they commit to the same policies as the other member states.\textsuperscript{82} Member country representatives now meet each December in Vienna, Austria to make deci-

\textsuperscript{73} See Pyetranker, supra note 67, at 157 ("Multilateral efforts to tackle cybercrime, cyber crises, and the export of cyber technology illustrate the seriousness with which world leaders treat cyberspace.").

\textsuperscript{74} See Pasko, supra note 8, at 345 ("Limiting the enforcement of encryption regulations to the United States will do little to deter terrorists or criminals from using encryption as long as those individuals can obtain such material from other industrialized nations.").

\textsuperscript{75} Id. at 345–46 ("[A]llowing a rigid encryption export regime punishes American companies because as these companies comply with tight regulations, their foreign competitors gain market share at their expense.").

\textsuperscript{76} Id. at 346.

\textsuperscript{77} Pyetranker, supra note 67, at 159.

\textsuperscript{78} Id. See generally The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, https://www.wassenaar.org/ (last updated Dec. 20, 2017) [hereinafter Wassenaar] [https://perma.cc/CMN3-J2EC].

\textsuperscript{79} Wassenaar, supra note 79; Pyetranker, supra note 67, at 160.

\textsuperscript{80} Wassenaar, supra note 79.

\textsuperscript{81} Pyetranker, supra note 67, at 161; Wassenaar, supra note 79.

\textsuperscript{82} Pyetranker, supra note 67, at 161–62; Wassenaar, supra note 79.
The Wassenaar Arrangement website provides this purpose statement:

The Wassenaar Arrangement (WA) has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. The aim is also to prevent the acquisition of these items by terrorists. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.84

The United States’ EAR controls over the export of encryption items is “[c]onsistent with our international obligations as a member of the Wassenaar Arrangement.”85 United States and international export controls impact defense industry company transactions involving encryption, encrypted items, and sensitive information.

IV. Encryption, Sensitive Information, and the Defense Industry

Encryption plays many roles within the defense industry. Companies develop software for use in manufacturing certain products that include encryption; encrypt the transfer of sensitive information to parties outside of their company and the United States; and require their employees travel with company laptops and cellphones that include encryption properties.

United States export control laws regulate encrypted items. Defense industry companies also export encrypted items and encryption technology to international customers including foreign governments and companies incorporated in foreign countries. United States Defense Industry companies selling their products, services, and data to foreign companies and governments must follow the government export regulations.

Compliance with these regulations requires a tedious order of review to determine which jurisdiction of regulations each item falls under. Items manufactured for the defense industry fall under the ITAR, and dual-use items (those items not specifically designed for a military application and with commercial uses) fall under the jurisdiction of the EAR. After determining jurisdiction, proper classification of an item is required. The ITAR regulates items found on the USML. The EAR regulates items found on the CCL. These lists are long and detailed and determining the correct classification of an item requires

83. Wassenaar, supra note 79.
84. Id.
a complete understanding of the item, its uses, capabilities, the end-user, and end-use. Once a company determines the correct jurisdiction and classification of an item, it must then determine whether or not the item requires approval from a United States government agency for export to its foreign end-user.

If approval is required, a company must submit an application for an export authorization to the Department of State for the export of items governed by the ITAR or the Department of Commerce for the export of items governed by the EAR. Exporters must wait for agency approval before exporting the product. Additional requirements such as shipment tracking, record keeping, reporting, and other limitations may apply when using an approved export authorization.

Transfer of sensitive information is susceptible to unauthorized releases and data hacking; defense industry companies can protect information with cybersecurity measures including the use of encryption.

A. Sensitive Information

Exporters can use defense industry encryption strategies to protect information and technology. Sensitive company information includes intellectual property, trade secrets, research and development, new technologies, personal employee information, customer lists, etc. For defense industry companies, the risks of cybercrime impact national security, economy interests, foreign policy and treaty compliance, and United States technology leadership.

Cybersecurity is multifaceted within the defense industry. Data saved on employee laptops related to their work, whether classified or unclassified, technical data, or proprietary information, is at risk of cyberattack. Employees need computers and cellphones to conduct business, but access to the internet puts company secrets at risk. Use of email, opening documents from unknown senders, sending documents to recipients who are not authorized to receive the documents, and traveling internationally with company assets are all risk areas for defense industry companies to consider.

Phishing is a form of data hacking used to obtain passwords and information, including military and financial data by phishers posing as a trust-worthy source in an e-mail. Spear phishing is much more targeted because a phisher will use information in an email, such as names and relevant language, to create the appearance of legiti-

86. See id. § 730.7.
87. Id. § 762.
88. See Shelton & Johnson, supra note 9.
89. 15 C.F.R. § 730.6; see generally 22 C.F.R. § 120 (2017).
macy.91 Hackers use regular phishing in identity theft attempts, but spear phishing “on government systems is usually an attempt to gather information and intelligence.”92 A spear phisher will send a link or attachment hoping the email recipient will open it so the phisher’s “malicious logic” will download, providing access to data that the phisher seeks.93 Employees should use digital signatures and encrypted emails when connected to the company’s network.94 Personnel in the defense industry, whether military or civilian, should utilize encrypted emails that are password protected in their correspondence. When internal users and trusted outside contacts both use encrypted emails, the risk of successful phishing and spear phishing attempts is minimized.

Another cybersecurity threat defense industry companies must address is the insider threat. Defense industry companies routinely give employees, contractors, and other agents working for a defense industry company the access to company information. This act leaves companies vulnerable to misconduct, whether intentional or unintentional. For example, third parties may approach employees to steal company information for a profit, but more commonly, employees do not safeguard their passwords effectively or do not practice secure transferring methods, allowing them to get into the wrong hands.95

Cyberattacks may also occur for personal hackers to display their skills, to promote particular causes, or to produce a profit.96 Defense industry employees expose companies to additional risks when they use company assets on international travel.

B. Employees Traveling Internationally

Defense industry companies sending employees overseas increase “the risk of unauthorized access to United States controlled information, including sensitive network data and data critical to the United States domestic communications infrastructure.”97

Many defense industry employees with international customers and partners are required to travel outside of the United States to conduct business. It remains no surprise that these employees will take their company issued laptops and cellphones with them during business

91. Id.
92. Id.
93. Id.
94. See id.
96. Finnemore & Hollis, supra note 9, at 434–35.
travel. Defense corporations should monitor employee travel to ensure compliance with export regulations.

Employees traveling internationally with company assets may not only require an export authorization for the laptop, cellphone or other asset but may also require additional authorization to take certain information stored on the asset. The BIS ENC exception may be used as authorization for the majority of company assets traveling overseas with employees.98

The United States government has reasons for so closely regulating the export of encryption technology and encrypted items. However, different sides of the debate argue about the level and intensity of regulations.

V. THE REGULATION DEBATE

A. The Problem with Regulations

United States exports regulations “are at the center of the debate over whether or not strict controls on encryption exports actually increase national security.”99 Some critics argue that strict regulations result in lost revenues for United States companies because, at least in the past, other countries allowed for the export of stronger encryption technologies.100 Although intended “to promote economic growth and strengthen national security,” export control regulations “have actually damaged America’s national security by hampering its technological growth.”101

The United States used to be the leader in encryption technology and America’s allies were once willing to follow our lead.102 However, “[s]ince the end of the Cold War . . . America’s traditional allies have little to gain by following America’s notions of national security.”103 Competing countries no longer “see America’s global economic and political power as a reason to follow the American lead, but rather, they view it as a challenge to compete more robustly in the international marketplace.”104 The United States must now attempt to collaborate with other countries on global security efforts because collaboration both helps the United States and the entire international community.105

With recent export control reform and a push for additional updates, the United States is “easing the restrictions on the export of encryption technology” which will allow the United States “to work

99. Pasko, supra note 8, at 339.
100. Id. at 340.
101. Id. at 337–38.
102. Id. at 350.
103. Id.
104. Id.
105. Id.
with other countries in establishing an effective encryption export regime.” 106 Continued regulation changes and collaboration with other countries is also necessary for more efficient encryption exports. 107

However, “[a]s a consequence of encryption’s success and widespread use, the United States is faced with the challenge of balancing its need to compete economically by ensuring its encryption products are widely available in foreign markets while at the same time protecting its national security interests.” 108

Current international collaborations are not without their faults. Critics of the Wassenaar Arrangement assert that the restriction of encryption exports violates free speech rights because “coded language communications are protected as a right of free expression under the International Covenant on Civil and Political Rights, to which most members of the Wassenaar are parties.” 109 Another side of the debate asserts that the Wassenaar Arrangement does not enforce rules adequately and does not bind any member state to its policies since no penalty exists for failing to enforce laws. 110 The Wassenaar Arrangement is seen as just a group of member states exchanging information on export controls but is not a real governing authority to enforce the organization’s goals. 111 International attempts to keep encryption technology within the control of member nations as the technology advances and has the ability to cross boundaries so easily remains challenging despite criticism. 112

The risks to national, business, and personal security may require some control over the international exchange of information and technology.

B. The Need for Regulations

Encryption technology and data stored on encrypted items are exported from the United States to foreign persons, companies, and governments every day. While these transfers may be a part of fulfilling business contracts, the United States government is interested in securing the information and technology exchanged. The government asserts some control over the export of these items to ensure the safety of this information and technology. The government will also investigate when information and items are hacked or stolen.

In 2015, Executive Assistant Director of the Science and Technology Branch of the Federal Bureau of Investigation (“FBI”), Amy Hess, issued a statement on Encryption and Cyber Security for Mobile

106. Id. at 351.
107. See id.
108. Id. at 339.
109. Id. at 341.
111. Id. at 168.
112. Id. at 170.
and Electronic Communication Devices.\footnote{113} In her statement, Hess addressed continually evolving national security and criminal threats that require the FBI to constantly question whether it is addressing those threats effectively.\footnote{114}

Hess asserted that security and cybersecurity threats continue to grow, and the FBI must adapt “to stay ahead of changing threats and changing technology.”\footnote{115} The FBI recognizes that the United States is interested “in promoting innovation and the competiveness of United States companies in the global marketplace, as well as freedom of expression around the world.”\footnote{116} However, when ensuring national security and seeking justice for cybercrimes, law enforcement has two issues to deal with: First, “legally authorized real-time interception of what we call ‘data in motion,’ such as phone calls, e-mail, text messages and chat sessions in transit.” Second, “legally authorized access to data stored on devices, such as e-mail, text messages, photos, and videos—or what we call ‘data at rest.’”\footnote{117} Both of these data areas are “increasingly encrypted.”\footnote{118}

The government must access information to investigate properly, but most communication services companies no longer “have the ability to isolate and deliver particular information when ordered to do so by a court.”\footnote{119} Unencrypted metadata, “is incomplete information” and “difficult to analyze when time is of the essence.”\footnote{120} Stored data is not a new frontier for government officials, but advancements to the technology, including automatic encryption settings with stronger encryption on devices and networks, make it increasingly difficult for law enforcement to gather information.\footnote{121} For example, communication services companies sell encryption technology that even they cannot decrypt.\footnote{122} This seemingly bulletproof system may be advantageous to a user wanting to secure personal information from

\begin{flushleft}

114. \textit{Id.}

115. \textit{Id.}

116. \textit{Id.}

117. \textit{Id.}

118. \textit{Id.; see also} Shaw, \textit{supra} note 13 (“The upswing in the use of powerful encryption to protect data-at-rest (data stored on a device such as a computer, mobile device, external hard drive, or USB stick) and data-in-motion (data being sent from one device to another over mobile towers, the Internet, or another network) is the direct result of people reacting what Edward Snowden revealed to the world in May 2103: U.S. government agencies routinely spy on everyone, including American citizens.”).


120. \textit{Id.}

121. \textit{Id.}

122. \textit{Id.}
\end{flushleft}
everyone, even the government, though “the reality is that cyber adversaries will exploit any vulnerability they find.”

The FBI also recognizes the need to secure information from United States adversaries by using advanced encryption technology and more secure networks, but it also recognizes that “absolute security does not exist in either the physical or digital world.” If a cyberattack occurs and the FBI is unable to access encrypted information or systems, it “may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets.”

In the past, communications services companies produced devices that allowed law enforcement to decrypt a device or program; however, now only limited information may be retrieved, making it “increasingly difficult” for the FBI to “investigate and prevent crime and terrorist threats.” If this becomes the norm, it will be increasingly difficult for us to investigate and prevent crime and terrorist threats.

Where some citizens may prefer the government to be less involved, others recognize a “need not only for tougher sentencing for criminals who use encryption to commit and hide their illegal activity, but also for more sophisticated measures to prevent these crimes from occurring in the first place.”

Advancing technology in other areas presents more complex challenges for regulating agencies and law enforcement. For example, the entrance of AI and machine learning technology has alerted government officials to predict security issues and to anticipate malicious use for any new technological advancement. Specifically, the use of AI technology may result in cyber threats exceeding what human hackers can currently accomplish. Although machine learning offers technological advancement that would benefit the defense industry, it could also make the defense industry more vulnerable to cyberattacks. Red Teams are becoming more commonplace within the cybersecurity community and are implemented to discover breaches in information systems that can be susceptible to cyberattack.

123. Id.
124. Id.
125. Id.
126. Id.
127. Id.
128. Id.; Pasko, supra note 8, at 347.
130. Id.
132. Id.
The United States government recognizes the need for cybersecurity to protect its products, technology, and information, and it implements regulations in an effort to protect those products. Defense industry companies must develop programs to comply with government regulations.

VI. DEFENSE INDUSTRY COMPLIANCE WITH REGULATIONS

A. General Government Guidance

Companies in the defense industry must ensure that they comply with United States export regulations and statutes related to the export and use of encrypted items. Additionally, companies should be aware of the risks to sensitive and export controlled information, such as ITAR technical data and EAR technology, and take action to protect that information.

For instance, the State Department’s Office of Defense Trade Controls Compliance (“DTCC”) issued “Compliance Program Guidelines” (DTCC Guidelines) to assist defense industry companies. The Department of Commerce, Bureau of Industry and Security issued its own “Export Compliance Guidelines: The Elements of an Effective Compliance Program” (BIS Guidelines).

The DTCC Guidelines state that companies involved in the export of items controlled by the ITAR should develop a “[c]omprehensive operational compliance program” which should “include manuals that articulate the processes to be followed in implementing the company program.” The BIS Guidelines distinguish eight elements of an effective compliance program: management commitment, risk assessment, export authorization, recordkeeping, training, audits, export violation correction, and export compliance program establishment and maintenance. The DTCC Guidelines and the BIS Guidelines are similar and good resources for defense industry companies when creating and maintaining effective compliance programs.

The DTCC Guidelines specify that the components of an effective compliance program include the following: (1) implementing an “Organization Structure” with charts, descriptions, and management structures indicating the company’s trade functions; (2) and tracking the compliance of United States export controls. The structure of the organization should be readily available to all employees, and it should provide the information for responsible parties within the com-

135. DTCC Guidelines, supra note 134.
136. BIS Guidelines, supra note 135, at 1.
137. DTCC Guidelines, supra note 134.
pany and include their titles and individual responsibilities. Senior management should make a corporate commitment to follow United States export control regulations and create and implement a company policy that is aligned with those regulations. Senior management should also emphasize for all employees the importance of compliance with United States export control regulations and define each employee’s individual role in helping the company maintain compliance.

Management should devote adequate resources to compliance matters and elect senior executives to complete everyday export and import operations and compliance management. Each business area and department should have its own operating procedure for handling export and import compliance matters.

Defense industry companies should also track the movement of export controlled items from the time of manufacture or purchase to the time of export. Compliance officers should consider employee knowledge of export regulations, how this knowledge applies to the employees’ daily tasks, who to contact with assistance in exporting items or information, recordkeeping requirements, and any changes to regulations.

Compliance officers should also ensure that employees are aware of regulation requirements for the subsequent retransfer of exported items controlled by regulations. Compliance programs should include procedures for screening parties that are restricted from export and any high-risk transactions.

Export control regulations require recordkeeping for years after use of export authorizations, and compliance programs should include procedures for maintaining and reviewing these records. The programs should conduct additional review to ensure compliance measures are effective and no violations have occurred; in addition, the programs should perform self-assessments and audits regularly to assess high-risk areas and any areas within the company that could use improved or updated compliance training, procedures, or other changes.

138. Id.
139. Id.
140. Id.
141. Id.
142. Id.
143. Id.
144. Id.
145. Id.
146. Id.
147. Id.
Compliance programs should also maintain training programs for employees to understand compliance requirements. When issues do occur, employees should know who to report suspected violations to within the corporation and how much supporting evidence to provide regarding the violation.

The DTCC and BIS Guidelines offer high level guidance on implementing and maintaining a compliance program. However, these programs must attempt to balance business requirements, comply with regulations, and adapt to changing regulations and technology.

B. Compliance Programs in Action

In November 2017, the former Acting Director for the DTCC, Arthur Shulman, provided the defense industry with some outgoing guidance on compliance with export control regulations. He recommended reporting any data hacking instance to the DTCC as a potential unauthorized export of export controlled information. Shulman stated that export controlled information is presumably released during a hack, unless it can be proven otherwise. To protect export controlled information, Shulman stated that companies should “(1) Know what you have (proper classification); (2) Know where you have it; and (3) Know who has access to it.”

When investigating issues with export controlled information, defense industry trade compliance personnel should work with IT and security personnel within their company to gather details and resolve issues. Trade compliance personnel should utilize internal databases and other IT systems to mitigate and correct as part of the investigation and voluntary disclosure drafting process.

Defense industry companies must implement compliance programs that are effective in ensuring their employees understand their role in export control compliance. It is easier to approach training from a teaching standpoint, with lecture-style courses and quizzes to test understanding, but it is far more effective to train employees to change their behaviors. Training should frame the information to instruct

---

149. Id.
150. Id.
151. Id.
152. Id.
153. Id. ("Trade Compliance personnel should be included in IT security incidents involving Export Controlled Data... IT security personnel should be included in Trade Compliance incidents involving IT systems.").
154. Id. ("When drafting Voluntary Disclosures involving electronic data, make sure IT is engaged. Leverage IT resources in the investigation, make sure controls are accounted for in the SSP, and corrective actions defined/planned/implemented through the POA&M.").
employees what they need to do habitually as part of their daily tasks instead of trying to impart abstract legal concepts.\textsuperscript{156} Compliance officers have the responsibility to understand the regulations well enough to synthesize procedural steps adaptable to all types of employees and job functions.\textsuperscript{157} Relying on employees’ memorization in a regularly scheduled training plan may be easy for compliance officers, “but it makes actually complying incredibly difficult for employees.”\textsuperscript{158} Essentially, effective compliance training begins with recognizing that employee norms need to change, and that process begins with behavioral changes, not teaching advanced concepts.\textsuperscript{159}

Compliance programs are constantly challenged to keep up with advancing technology and changes to regulations while also ensuring all employees understand their individual roles in maintaining compliance and securing company information.

\section*{VII. Advancing Technology}

\subsection*{A. Regulation Reform}

BIS issued a final rule that went into effect on September 1, 2016, as part of the Departments of Commerce and States’ initiative to reform export control regulations.\textsuperscript{160} The final rule states:

\begin{quote}
Transmitting or storing electronic data that meet certain security standards would not constitute an export of that data, provided that the technology or software is: (1) Unclassified; (2) Secured using “end-to-end encryption”; (3) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current United States National Institute for Standards and Technology publications, or other equally or more effective cryptographic means; and (4) Not intentionally stored in a military-embargoed country or in the Russian Federation.\textsuperscript{161}
\end{quote}

Because of this final rule, the EAR now includes a definition of “end-to-end encryption” which is “(i) the provision of cryptographic protection of data such that the data are not in unencrypted form be-

\begin{itemize}
\item \textsuperscript{156} \textit{Id.}
\item \textsuperscript{157} See \textit{id.} (“Instead of taking training on a scheduled basis and hoping you remember it, effective training builds itself into the business process where the behavior takes place.”).
\item \textsuperscript{158} \textit{Id.}
\item \textsuperscript{159} \textit{Id.}
\item \textsuperscript{161} \textit{Id.; see generally}, Information Technology Laboratory, \textit{supra} note 24.
\end{itemize}
between originator (or the originator’s in-country security boundary) and an intended recipient (or the recipient’s in-country security boundary); and (ii) the means of decryption are not provided to any third party.”

Access information in the EAR is now defined and includes things like “decryption keys, network access codes, and passwords.” According to this rule, any victim of an encrypted data breach will not be found responsible for the transfer of the data so long as the person sending the EAR controlled information withheld access information to the encrypted data. Defense industry companies will certainly benefit from these more relaxed rules, at least in terms of EAR controlled technology, but it must keep in mind that this final rule for the EAR does not apply to ITAR controlled technical data.

On April 12, 2018, the House Financial Services Monetary Policy and Trade Subcommittee completed its last hearing on a bill to “broaden the authority of the Committee on Foreign Investment in the United States (CFIUS)” on business arrangements between the United States and foreign parties and the transfer of sensitive technology. A representative for the technology industry stated that the current export control system is the correct method for governing sensitive technology transfers. The bill drafter, Representative Robert Pittenger, criticized current export control regulations for its failure to prevent China from acquiring United States technology.

The House Foreign Affairs Committee introduced a bill in February of 2018 “to renew the legislative basis for United States dual use export controls for the first time in nearly twenty years.” The Export Control Reform Act (ECRA) “offers both risks and rewards for U.S. and non-U.S. companies with an interest in United States technology exports. U.S. subsidiaries of non-U.S. companies should watch the bill closely, as the current legislative test treats them as “foreign persons” and could restrict their ability to exchange technology with other United States companies.”

162. Schwechter, supra note 161.
163. Id.
164. Id.
165. Id.
167. Id.
168. Id.
170. Id.
The results of ECRA could strongly affect controls and technology development for United States companies working in technologies such as advanced aerospace. Current processes for determining items that require control under the regulations have improved recently, but the regulations still need to be modernized to capture new technologies. Additionally, some regulations make it difficult for defense industry companies to comply and conduct business without increasing national security. The proposed ECRA would replace the Export Administration Act (“EAA”) “with legislation that does not require regular re-approval by Congress.” It would give the President authority to control exports, re-exports, and transfers of items by persons anywhere in the world.

In 2011, President Barack Obama instituted the New International Strategy for Cyberspace to produce the following:

“[A]n international environment that ensures global networks [is] open to new innovations, interoperable the world over, secure enough to support people’s work, and reliable enough to earn their trust. To achieve it, we will build and sustain an environment in which norms of responsible behavior guide states’ actions, sustain partnerships, and support the rule of law.”

These norms include: “Upholding Fundamental Freedoms, Respect for Property, Valuing Privacy, Protection from Crime, Right to Self-Defense, Global Interoperability, Network Stability, Reliable Access, Multi-Stakeholder Governance, [and] Cybersecurity Due Diligence.”

The United States recognizes the need to not only govern and regulate exports of products, information, and technology but also to adapt regulations that reflect advancements in technology and the need for defense industry companies to implement strong cybersecurity defenses. Defense industry companies are also challenged to keep up in an ever-evolving cyber world.

B. Keeping Up in the Defense Industry

With encryption technology advancing beyond the pace of policy publication, defense industry companies must not only abide by relevant regulations but should take concerted action to protect against

171. Id.
172. Id. at 2.
173. Id.
174. Id. at 3.
Our reliance on cyber technology exposes individuals and companies to new risks related to the protection of information.178 Currently, cyber-crime “may be the greatest threat to every company in the world.”179 It is estimated that cyber-crime costs the global business industry hundreds of billions of dollars each year, and by 2019 that number will increase to approximately $1.2 trillion.180 This increase can be attributed to the “rapid digitization of consumers’ lives and enterprise records” and to the production of more professional and successful cyber-attacks.181 “[C]ybersecurity concerns that were once primarily about data security, privacy[,] and free speech are now concerns about (1) human safety and (2) the operational preservation of industrial and financial infrastructure.”182

Data breaches are becoming more common, and they can affect a company’s reputation. However, companies statistically rely heavily on third-parties providing them access to the company’s networks and systems.183 To keep up with advancing technology and increased reliance on third-party vendors, companies should mitigate risks by relying on automated processes to manage access to databases, which will save time and delay business but still ensure security for sensitive company information.184 Defense industry companies should be aware of the issues involved with controlling the technology, regulating export of the technology, and reacting to data hacking events.

Earlier this year, a global software company was charged with violating United States regulations in the release of export controlled information and access to sensitive data.185 The software company settled and agreed to implement an “Enhanced Security Plan” which includes security enhancements and requirements.186 Some examples

177. See Pyetranker, supra note 67, at 153 (“[C]oncerted action—rather than passive pessimism—must be our response to cyber threats.”).
178. Id. at 155 (“All the benefits of living in a networked society are, however, tempered by concomitant risks. In addition to the familiar perils of warfare, crime, espionage, and terrorism, new threats of cyber-warfare, cybercrime, cyberespionage, and cyberterrorism have emerged. In the brave new cyber-world, these dangers and others are poised to exploit our reliance on e-lifestyles.”).
181. Morgan, supra note 180; Seffers, supra note 181.
183. See Bomgar, supra note 96.
184. Id.
185. LeCour, Carlile, & Chin, supra note 98.
186. Id.
of these requirements include: restricting and controlling access by U.S. and non-U.S. persons; implementing a security policy; and appointing a Security Director to ensure compliance with United States regulations and company policies.\footnote{187}{Id.}

In addition to adopting measures to answer current regulations, companies should consider and prepare for technological advancements and regulation reforms. Technologies may advance and regulations may change, but how people respond to change is also a factor.\footnote{188}{Finnemore & Hollis, supra note 9, at 429 (“States and other stakeholders thus need to think more carefully than they have to date about how norms evolve, spread, and affect behavior.”).}

Hess’s sentiments in 2015 regarding encryption technology are still a concern for government officials today, and they are taking action.\footnote{189}{See Hess, supra note 114.} In response to Apple and Google announcing that they would strengthen their encryption products in 2014, former FBI director, James Comey, stated that “end-to-end encryption prevents law enforcement from collecting electronic evidence required to keep America safe.”\footnote{190}{Jack Karsten & Darrell West, TechTank: A Brief History of U.S. Encryption Policy, BROOKINGS (Apr. 19, 2016), https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/ [https://perma.cc/M7S9-XNLP].} Comey and other government officials, like their predecessors, seek to require “backdoors” into encryption products for the government.\footnote{191}{Id.} Unlike previous calls from the government for access to encrypted communications, these newer requests emphasize terrorism as the reason for the requested access.\footnote{192}{Id.}

On April 24, 2018, Lieutenant General Paul Nakasone was confirmed as the new Commander of the United States Cyber Command and the director of the National Security Agency.\footnote{193}{Brandon Knapp, Senate Confirms New Head of Cyber Command, NSA, FIFTHDOMAIN (Apr. 24, 2018), https://www.fifthdomain.com/dod/2018/04/24/senate-confirms-new-head-of-cyber-command/ [https://perma.cc/QQ9T-L5LJ].} Nakasone’s approach towards cyber security is described as “hawkish” but approved by Congress.\footnote{194}{Id.} Nakasone is replacing Admiral Michael Rogers who retires after serving almost four years in the position.\footnote{195}{Id.} Previously, Nakasone served as the general of United States Army Cyber Command and controlled the United States Cyber Command’s joint Task Force ARES, which assisted the military in combating the Islamic State group.\footnote{196}{Id.} With the confirmation of Nakasone, Cyber Command intends to be elevated to “a fully combatant command.”\footnote{197}{Id.}
Concurrent with Nakasone’s win, calls for new legislation to create a backdoor into encryption are coming forward once again.¹⁹⁸ These “surveillance hawks” include FBI director Christopher Wray and Senators Dianne Feinstein and Richard Burr.¹⁹⁹ However, privacy advocates reject the idea of unlocking devices for government investigation even though surveillance hawks state they are specifically concerned about access to devices used for criminal or terrorist activity.²⁰⁰ Encryption product manufacturers fight the requests for a government backdoor because “compromised encryption standards would reduce their ability to compete in the international market.”²⁰¹

When the United States government decides to update export control regulations or amend the Export Control Reform, defense industry companies must adapt their processes and procedures to reflect the changes within a timely manner. In 2013, the intention behind Export Control Reform was to allow more flexibility when exporting items that are of less concern to national security.²⁰² However, any change to export controls requires an overhaul of export compliance measures for defense industry companies. In changing the processes and procedures to reflect the reform, it may take considerable time and manpower—specifically, changing the norms for employees who are accustomed to conducting business a certain way for many years.

Recent Export Control Reform related to the export or transfer of EAR controlled encrypted technology allows companies to use a variety of “cloud computing and cloud storage solutions” that were not permissible in the past.²⁰³ Although the rules may provide more options for the use and transfer of encrypted data, defense industry companies must continuously implement security measures.²⁰⁴ Additionally, the changes to the EAR are not mirrored in the ITAR; therefore, defense industry companies especially must distinguish between EAR controlled technology and ITAR controlled technical data when using cloud services for storage and transfer.²⁰⁵ Changes to export control regulations provides the opportunity for defense industry companies to reassess their compliance programs.²⁰⁶

¹⁹⁸ Shaw, supra note 15 (“The Feinstein-Burr bill is only the most recent entry into [a] of attempts to make encryption backdoors for law enforcement the norm.”).
¹⁹⁹ Id.
²⁰⁰ Id.
²⁰¹ Karsten & West, supra note 191.
²⁰³ Schwechter, supra note 161.
²⁰⁴ Id.
²⁰⁵ Id.
²⁰⁶ See Schwechter, supra note 161 (“These rule changes represent an ideal time for companies to assess and update their export control compliance programs, and
VIII. Conclusion

The United States government is beginning to recognize the need for more advanced security measures to protect domestically produced technology and information, especially information that puts national security at risk. Specifically, the technology and information produced by United States defense industry companies should be protected from getting into the hands of our foreign adversaries at all costs. In response to the growing need for security measures, the United States government has implemented new programs, commissions, agencies, and projects to create more robust security systems and regulations. The United States should employ the most talented and experienced cybersecurity professionals to innovate and produce security systems that protect our nation’s most sensitive information. The government should then provide these systems to its defense industry companies at minimal cost and should require companies to use the best technology in its security measures.

With or without the government’s assistance, defense industry companies within the United States must also implement their own measures of protection. Current policies offer little protection of sensitive and export controlled information including encrypted items and information. In addition, the government should also provide the defense industry companies better guidance and access to resources in order to assist them in protecting the important information and encrypted items.\textsuperscript{207} For example, any new systems or software purchased by the United States should be made available to defense industry companies as the standard. If the government truly wishes to protect its most important technology and information, it should provide the new systems at minimal cost to the defense industry. Advancements in security programs should be shared with defense industry companies as soon as they are available and ready for use. Nevertheless, the government may not want to provide defense industry companies with the best security technology because in the event that the government needs to conduct an investigation, a company utilizing strong cybersecurity and encryption software is much more difficult to investigate.

Alternatively, the United States could update current regulations to require that defense industry companies must utilize specific security measures or face a penalty for failing to do so. Such regulation could require defense companies to implement more robust security programs with updated security software. This is a less effective solution

determine whether they can avail themselves of the new provisions regarding technical data and software.”).

\textsuperscript{207} See DeNardis & Raymond, supra note 183, at 495–6 (“Many firms deploying cyber physical systems are not, at least historically, technology firms. They have little experience with the existing legacy mechanisms for Internet governance, and in many cases may have little or no experience with multistakeholderism as a governance modality.”).
as the advancement in cyberattack technology increases so rapidly, and reformed regulations will likely be outdated as soon as they are implemented. It makes more sense to require that defense companies must implement the most updated software and programs determined by government security experts and cyber-security experts. Also, by allowing defense companies to decide which security companies it will work with, the defense companies obtain the option to shop for the best and most expensive program, or the company could choose the cheapest option, resulting in less efficient security. Cybersecurity regulations that are too specific run the risk of being outdated quickly, whereas broad requirements leave the option for companies to implement the lowest of security measures.

Even if the government declines these suggested measures, defense industry companies should make the protection of their sensitive information and encrypted items top priority. This method would require complete buy-in from the senior management within the company and a thorough flow-down of cultural beliefs among its employees. A change in norms must be implemented, and defense industry personnel should be inundated with reminders on the importance of information security. Companies should provide employees with easy access to guidance, training, and assistance in handling, sharing, protecting, and exporting sensitive and export controlled information. Changing company culture takes time, and failure to change personnel beliefs will result in a lack of understanding and potential violations of export control regulations. In the worst cases, data spills and cyberattacks could result in the loss of sensitive or even classified information that could jeopardize national security. Huge unauthorized data releases of sensitive information will negatively affect a company's reputation thus affecting its ability to generate revenue.

The risks in using and exporting encryption technology and sensitive information should be a major concern for defense industry companies. This concern should motivate the government to invest significant resources into compliance programs. Resources such as dedicated and qualified personnel can create policy and procedure to ensure compliance with United States government regulations, and the procedures will provide guidance and training to all employees. In addition, companies should employ IT security, data security, and counterintelligence personnel to work with the compliance team in innovating preventive measures and in addressing any potential data releases and export violations. Immediate actions and counter measures should be prioritized not just among the compliance and security teams but should be a known, expected response from all employees. In other words, cybersecurity norms should be instilled company-wide and thoroughly policed from within the company. How a company chooses to implement such measures remains discretionary, but a better resourced compliance department dedicated to implementing ef-
fective policies and responding quickly to potential issues will prevent export control violations and data releases of important information.

Defense industry companies transfer export controlled information that may subject the United States to security risks. The United States responds to this risk by implementing regulations to control the high-risk exports. Defense industry companies must comply with these regulations. Therefore, defense industry companies should approach exports and cybersecurity from the standpoint that technology is always advancing—failure to simultaneously advance security and compliance measures will leave the country and the company vulnerable to attack.