July 29, 2015

Mr. Anthony Dearth
Deputy Assistant Secretary
U.S. Department of State
Directorate of Defense Trade Controls
Compliance & Registration Division
2401 E Street NW, SA-1, Room H1200
Washington, DC 20522-0112

ATTN: ITAR Amendment—Revisions to Definitions; Data Transmission and Storage (RIN 1400-AD70)

Dear Mr. Dearth,

The Texas Public Policy Foundation's Center for the American Future has deep concern regarding the United States Department of State's (State Department) proposed Amendment to the International Traffic in Arms Regulations (ITAR). RIN 14000-AD70, June 3, 2015 (Proposed Rule). The Proposed Rule goes beyond its stated purpose—criminalizing the disclosure of basic firearm technical details (itself a dangerous overreach)—to criminalizing a wide range of speech posing no national security threat. By its literal terms, the proposed rule applies to technology not typically associated with weaponry, such as engines, fertilizer, and general engineering principles. The discussion of this technology on the Internet or many other public forums would be criminalized as "exportation" of "technical data." The State Department's proposal would unnecessarily restrict speech, hinder technological development, and interfere with advertising. That is not merely unwise policy; it is a violation of the First Amendment to the United States Constitution.

EXECUTIVE SUMMARY

In an effort to keep American military technology from foreign military forces, the State Department has promulgated a complex set of regulations that prohibit the "export" of "technical data" about "defense articles." All three terms are already defined broadly enough to prohibit the export of information regarding virtually anything that can be used as a weapon. The State Department now seeks to broaden the scope of the regulations still further—far enough to encompass everyday technology that few would think regulated. Most problematically, the proposed rule would expand "technical data" to include information already known to the public but not specifically approved by a government agency (by narrowing the exception for information in the "public domain"). It also seeks to expand "export" to include discussion or posting on the Internet and other public forums. When combined with the already broad scope of the information subject to the ITAR that one cannot "export," these changes will criminalize a vast swath of the Internet.

ITAR controls information that is "required" for the "manufacture," "operation," or "development" of virtually any weapon or military vehicle. And one must know a great deal of information in order to manufacture or develop even a simple weapon, such as a hunting rifle or a bomb. Much of that information, including basic engineering principles, is fundamental to other industries that do not involve military technology. If there is any doubt about the current breadth of ITAR, note that the regulations already see fit to exclude academic materials from university courses. That implies that they control basic principles that are *not* taught in academic courses. The Proposed Rule seeks to expand this already overbroad regime to the Internet—even to information already on the Internet.

The State Department's solution to the overbreadth of its asserted authority is to require anyone who might think their speech is "technical data" to apply for permission to post it on the Internet or other public forums. Instead, that approach aggravates the existing constitutional objections to the ITAR by adding an unconstitutional prior restraint to a vague, overbroad, content-based restriction on speech.

A better solution would be to withdraw the Proposed Rule. If the State Department wishes to modify ITAR, it should focus on narrowing its scope to free American technological development from the threat of government harassment for valuable speech.

ANALYSIS

I. The Proposed Definitions of "Technical Data" "Defense Article" and "Export" are Broad Enough to Criminalize Discussion of Everyday Technology

ITAR criminalizes the "export" of "technical data" or "defense articles" without authorization from the government. *See* 22 C.F.R. § 127.1. And these words are defined broadly enough to encompass everyday technology not typically thought of as posing a military danger. The Proposed Rule seeks to expand them still further, to a scope that would criminalize much of the discussion on the Internet.

A. "Defense Article"

The list of items and technology considered "defense articles" are enumerated on the United States Munitions List (USML). The USML includes many military items, such as tanks, battleships and bombs, as well as "technical data" about them. 22 C.F.R. § 121.1 at Category IV-VII. But it also includes virtually every firearm imaginable—even single shot hunting or target rifles—as well as "technical data" about those firearms. *See Id.*, Category I at (a), (b), and (i). Only black powder muzzle-loaders and non-combat shotguns are excluded. Even more concerning, it contains an open-ended catchall provision, allowing the State Department to impose ITAR control over "Any article not enumerated on the U.S. Munitions List." *Id.,* Category XXI. This broad definition creates serious First Amendment and practical problems when combined with the proposed definitions of "technical data" and "export."

B. "Technical Data"

The breadth of the proposed definition of "technical data," extends the already broad list of "defense articles" into common, nonmilitary items. The proposed definition includes, "Information required for the development … production … operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article." Proposed 22 C.F.R. 120.10(a)(1). A great deal of nonmilitary information is required for the "production," of military equipment (to say nothing of "operation" and "development"). For example, the production of a tank requires information about how to make an engine, vulcanize rubber for tires, or improve the strength of steel. The production of a bomb may require information about manufacturing fertilizer that could be used to make the bomb. An improvement in making propellers for ships may be used for a battleship. Discussion of

these nonmilitary subjects could land Americans in federal prison if the Proposed Rule goes into effect.

The problem is exacerbated by the Proposed Rule's assertion that "technical data" can take almost any form: "Technical data may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information gleaned through visual inspection." Proposed 22 C.F.R. 120.10(a)(1). Under this definition, a photograph of an improvement a private citizen makes to an engine can be considered "technical data." So is his oral description of that information to a friend. And, he has "exported" that information if his friend is foreign or if his conversation is overheard by a foreign person who is not a citizen or permanent resident. If the information is shared publically online, he has exported it even if he was only intending to share it with American citizens.

Furthermore, the Proposed Rule removes the current definition's exclusion for "basic marketing information." This will endanger countless merchants who wish to use photos, detailed descriptions, or excerpts from instruction manuals to sell their lawful products.

C. "Export"

The Proposed Rule's definition of "export" includes putting the above-described information on the Internet since foreigners might access it. Proposed 22 C.F.R. 120.17(a)(7) (defining export to include "Making technical data available via a publicly available network (e.g., the Internet)"). Given the breath of the information considered "technical data" and "defense articles," innocent discussions on technical topics in Internet forums would be criminalized. If a model rocket hobbyist provides technical information on a forum on the Internet, and a State Department official believes that the information is required for production of an unmanned aerial vehicle, the hobbyist could be incarcerated for 20 years. *See* 22 U.S.C. § 2778(c), (e). If a reporter publishes an article on a new technical development constituting "technical data," he too could be imprisoned.

D. "Public domain"

The Proposed Rule's exception for information already in the "public domain" does not prevent these scenarios because that term is defined to only include information already approved by a federal agency. After defining public domain more broadly, the Proposed Rule makes the following exception: "Technical data or software, whether or not developed with government funding, is not in the public domain if it has been made available to the public without authorization from [the appropriate federal agency]." Proposed 22 C.F.R. 120.11(b). This modification requires every American to get the

federal government's permission before discussing a broad range of information, much of which can touch on matters of public concern.

Put together, these definitions cover so much speech that the State Department saw fit to exclude information "Concern[ing] general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution." Proposed 22 C.F.R. 120.6(b)(3)(iii). That implies that even the State Department thinks that such basic principles would be illegal to discuss online if they were not commonly taught in schools or were not released in a catalog course or associated teaching laboratory.

Few Americans would stop to consider that discussing improvements to their new hunting rifle online could land them in prison for twenty years. Fewer still could imagine that discussing an improvement to their car's engine, fertilizer, boat propellers, or basic engineering principles could do the same. Given the breath of the operative definitions, what assurance do Americans have that they will not be imprisoned for otherwise lawful speech?

II. The Proposed Rule Violates the First Amendment

The Proposed Rule's restriction on sharing data, ideas, and improvements in technology is (1) a content-based restriction on speech that is not narrowly tailored; (2) an overbroad restriction of speech; (3) unconstitutionally vague; and (4) an unconstitutional prior restraint. Any one of these problems would invalidate the Proposed Rule under the First Amendment, but the State Department has gone for the quadfecta.

A. The Proposed Rule is a Content-Based Restriction on Speech

As the Supreme Court has often explained, "[A]bove all else, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content." *See Police Department of Chicago v. Mosley*, 408 U.S. 92, 95-96 (1972). A speech restriction is "content based if it require[s] enforcement authorities to examine the content of the message that is conveyed to determine whether a violation has occurred." *McCullen v. Coakley*, 134 S. Ct. 2518, 2531 (2014) (quotation omitted). The Proposed Rule does just that. By regulating only speech that conveys "technical data" about "defense articles," the rule's application directly depends on the content of the speech in question. Indeed, the rule's explicit purpose is to suppress such speech in order to keep it out of the hands of foreign militaries.

As a content-based restriction, the Proposed Rule is presumptively invalid. *R.A.V. v. City of St. Paul*, 505 U.S. 377, 382 (1992). It can only withstand strict scrutiny if the

government proves it is narrowly tailored to serve compelling government interests. *Id.* at 395. That the State Department cannot do. While restricting our enemies' access to military technology is certainly a compelling government interests, this rule reaches far beyond such technology into everyday items and single-shot pistols—technology that would not aid even the most ill-equipped militants. Furthermore, the narrow definition of "public domain" means that even information already on the Internet but not approved by a government agency is covered by ITAR. Because foreign militaries have access to such information via alternate sources, restricting it does not advance the government's interest. In other words, there can be no compelling government interest in restricting publication of technical information that is already publicly available. The Proposed Rule is therefore not narrowly tailored.

B. The Proposed Rule is Overbroad

A rule is overbroad if "a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *United States v. Stevens,* 130 S. Ct. 1577, 1587 (2010). That is the case here. While the rule could be constitutionally applied to the exportation of certain military technology or weapons, it cannot be used to criminalize all speech on the Internet regarding the long list of items on the USML, along with any speech that may be "required" to "manufacture" or "develop" those items.

The Proposed Rule is particularly overbroad given that civil violations of ITAR have no *mens rea* requirement. In *Gorrin v. United States,* 312 U.S. 19 (1941), the Supreme Court upheld the Espionage Act because it only punishes those who act "with intent or reason to believe that [the information] is to be used to the injury of the United States, or to the advantage of any foreign nation." Relying on *Gorrin*, the Ninth Circuit has held that ITAR regulations must contain such a *scienter* requirement in order to avoid criminalizing protected speech. *See United States v. Elder Industries,* 579 F. 2d 516 (9th Cir. 1978). Without such a limitation, the Proposed Rule cannot be compatible with the First Amendment.

C. The Definitions of "Defense Article" and "Technical Data" are Unconstitutionally Vague

Consistent with the Fifth Amendment, the government may not create ill-defined crimes. "It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined." *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). Vagueness doctrine applies with particular force when the government attempts to restrict speech. "[S]tricter standards of permissible statutory vagueness may be applied to a statute having a potentially inhibiting effect on speech; a man may the less be

required to act at his peril here, because the free dissemination of ideas may be the loser." *Hynes v. Mayor & Council of Oradell*, 425 U.S. 610, 620 (1976) (quotations omitted). Freedom of speech is "delicate and vulnerable, as well as supremely precious in our society. The threat of sanctions may deter their exercise almost as potently as the actual application of sanctions." *NAACP v. Button*, 371 U.S. 415, 433 (1963). "Because First Amendment freedoms need breathing space to survive, government may regulate in the area only with narrow specificity." *Id*. The Proposed Rule flouts these considerations.

As described above, the definition of technical data may include anything "necessary" for the production of any article on the USML, which itself is unlimited due to its catchall provision. 22 C.F.R. 121.1, Category XXI. In fact, the potential definition is so broad that the State Department found it necessary to exclude information "Concern[ing] general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution." Proposed 22 C.F.R. 120.6(b)(3)(iii). If algebra and physics need to be excluded from the definition of "defense articles," these regulations are potentially limitless. The State Department has not adhered to the precision required when attempting to restrict speech, especially based on its content.

D. The Proposed Rule is an Unconstitutional Prior Restraint on Speech

The Department's solution to the broad and blurry scope of its regulations is to require government approval before speech can be put on the Internet. Instead of providing clear limits to the information that may not be discussed, the Department relies on the "commodity jurisdiction" regime, in which it grants permission to speak "if doubt exists." 22 C.F.R 120.4. That is not a solution but rather a prior restraint on speech—perhaps the most clearly unconstitutional of all speech regulations. *Southeastern Promotions, Ltd. v. Conrad*, 420 US 546, 558-59 (1975) ("The presumption against prior restraints is heavier—and the degree of protection broader—than that against limits on expression imposed by criminal penalties. Behind the distinction is a theory deeply etched in our law: a free society prefers to punish the few who abuse rights of speech after they break the law than to throttle them and all others beforehand.").

The term "prior restraint" is used "to describe administrative and judicial orders forbidding certain communications when issued in advance of the time that such communications are to occur." *Alexander v. United States*, 509 U.S. 544, 550 (1993). That is exactly what the commodity jurisdiction procedure does.

Acknowledging the lack of clear standards in its definitions of "defense articles" and "technical data," the State Department requires citizens to submit their proposed speech

for approval—for a "determination" of whether the information is subject to ITAR. 22 C.F.R 120.4. This process can take years, as even the State Department has difficulty applying its own standards. In the meantime, the free flow of ideas and research are halted. While the commodity jurisdiction procedure may be constitutional when determining whether objects and weapons may be exported, it is not constitutional when determining whether speech may be posted on the Internet.

1. Open-ended licensing

Open-ended licensing for speech is not permitted under the First Amendment. The Supreme Court has continuously held that "[I]n the area of free expression a licensing statute placing unbridled discretion in the hands of a government official or agency constitutes a prior restraint and may result in censorship." *City of Lakewood v. Plain Dealer Publishing Co.*, 486 US 750, 757 (1988). The government "cannot vest restraining control over the right to speak … in an administrative official where there are no appropriate standards to guide his action." *Kunz v. New York*, 340 U.S. 290, 295 (1951). Accordingly, standards governing prior restraints must be "narrow, objective and definite." *Shuttlesworth v. Birmingham*, 394 U.S. 147, 151 (1969). Standards involving "appraisal of facts, the exercise of judgment, [or] the formation of an opinion" are unacceptable. *Forsyth County v. Nationalist Movement*, 505 U.S. 123, 131 (1992) (quotation omitted). Given the vague definitions of "technical data" and "defense article," the open-ended commodity jurisdiction procedure does not satisfy these requirements and may therefore not be applied to speech.

2. Lack of procedural safeguards

The commodity jurisdiction procedure is independently unconstitutional because it lacks procedural safeguards against abuses of discretion. The following procedural safeguards are required of even content-neutral prior restraints:

- The burden of proving the speech may be regulated must rest on the censor;
- The determination must be prompt; and
- Judicial review must be available for all permit denials. *Freedman v. Maryland*, 380 U.S. 51, 58 (1965) ("Only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression.").

None of these procedural safeguards are available here. The State Department requires individuals to apply for permission to speak "if doubt exists" as to whether their speech falls under ITAR. 22 C.F.R.120.4(a). The determination can take years. For example, the State Department only ruled on the Defense Distributed's applications after being sued

for ignoring the applications for two years. *Defense Distributed v. United States Dept. of State*, No. 29, 15-CV-372-RP (W.D. Tex. June 8, 2015). And finally, the underlying statute purports to make the "designation…of items as defense articles" unreviewable in court. 22 U.S.C. 2778(h).

The broad prohibition on prior restraints is no less applicable in the area of national security. In *New York Times v. United States*, 403 U.S. 713 (1971), the Supreme Court rejected the government's authority to stop the publication of the Pentagon Papers—classified information pertaining to American military activities in the then-ongoing Vietnam War. In the face of that decision, the State Department cannot claim to have the authority to license the discussion of basic firearms, engineering principles, or engines online—even if it would help prevent the Islamic State from obtaining the latest in American deer rifle technology.

III. Congress Never Authorized the State Department to Ban the Dissemination of Information on Basic Technology

The statutory authority for the ITAR authorizes the President, "[i]n furtherance of world peace and the security and foreign policy of the United States . . . to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services." 22 U.S.C. § 2778(a)(1). To this end, "[t]he President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services." *Id.* From this statutory seed has already grown a regulatory jungle. The State Department's further suggestion—that this language also gives it the authority to regulate *the discussion* of any technology that might be used militarily or might be necessary to produce military technology—strains credulity. That is especially so given the numerous First, Second, Fifth, and Tenth Amendment problems with its proposed rule. *See Whitman v. American Trucking Assns., Inc.,* 531 U.S. 457, 468 (2001) (noting that Congress does not "hide elephants in mouseholes.").

IV. The Proposed Rule is Subject to Abusive, Discriminatory Enforcement

These constitutional considerations exist to protect the people form discriminatory enforcement and arbitrary prosecution. "Under the First and Fifth Amendments, speakers are protected from arbitrary and discriminatory enforcement of vague standards.'" *Nat'l Endowment for the Arts v. Finley*, 524 U.S. 569, 588 (1998) (citation omitted). The regulatory regime embodied in the Proposed Rule will not and cannot ban all of the speech it encompasses. Instead, it will be a weight hanging over the Internet, ready to

drop whenever the government finds speech it wishes to suppress or a speaker it wishes to imprison, and chilling the free expression of ideas in the mean time. Our Constitution does not tolerate such a regime, and neither should our government suggest one.

V. Conclusion

The State Department is not constitutionally permitted to muzzle the American people under the guise of keeping 19th Century technology out of the hands of terrorists and foreign militaries. The Proposed Rule leaves anyone who discusses technology not specifically approved by a federal agency vulnerable to 20 years in prison because a foreign person may overhear him or access the information on the Internet. That result is not consistent with the Constitution, basic principles of liberty, or even reasonable policy making.

The Texas Public Policy Foundation's Center for the American Future urges you to withdraw the Proposed Rule.

Sincerely,

ROBERT HENNEKE
Director, Center for the American Future

JOEL STONEDALE
Attorney, Center for the American Future

Texas Public Policy Foundation
901 N. Congress Avenue
Austin, Texas 78701