WILLIAM J. OLSON
(D.C., VA.)

JOHN S. MILES
(D.C., MD., VA. OF COUNSEL)

HERBERT W. TITUS
(VA. OF COUNSEL)

JEREMIAH L. MORGAN
(CA ONLY)

ROBERT J. OLSON
(VA.)

WILLIAM J. OLSON, P.C.
ATTORNEYS AT LAW
370 MAPLE AVENUE WEST, SUITE 4
VIENNA, VIRGINIA 22180-5615
TELEPHONE (703) 356-5070
FAX (703) 356-5085
E-MAIL: wjo@mindspring.com
http://www.lawandfreedom.com

114 CREEKSIDE LANE
WINCHESTER, VA 22602-2429
TELEPHONE (540) 450-8777
FAX (540) 450-8771

August 3, 2015
By email to DDTCPublicComments@state.gov

Office of Defense Trade Controls Policy
U.S. Department of State
Washington, DC

Re: Gun Owners of America, Inc. and Gun Owners Foundation Comments to U.S. Department of State, Directorate of Defense Trade Controls on: "International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions" (Public Notice 9149, 6/3/15)

Dear Sirs:

Our firm represents Gun Owners of America, Inc. ("GOA") and Gun Owners Foundation ("GOF"),[1] which submit these joint comments pursuant to the request for comments published by the U.S. Department of State ("State Department") on its proposed definition revisions and proposed new definitions to certain key terms of the International Traffic in Arms Regulations ("ITAR").[2] GOA and GOF appreciate that the State Department has provided this opportunity to comment on this topic.

[1] GOA is a national membership, educational and lobbying social welfare organization, devoted to protecting and defending firearms rights across the country. GOA was incorporated in California in 1976, and is exempt from federal income tax under section 501(c)(4) of the Internal Revenue Code ("IRC"). GOF is an educational and legal defense organization defending the Second Amendment of the U.S. Constitution. GOF was incorporated in Virginia in 1983, and is exempt from federal income tax under IRC section 501(c)(3). GOA and GOF are headquartered in northern Virginia.

[2] 80 Fed. Reg. 31525 (June 3, 2015), http://www.gpo.gov/fdsys/pkg/FR-2015-06-03/pdf/2015-12844.pdf ("Proposed Regs").

1. Overview.

The Arms Export Control Act ("AECA") (22 U.S.C. sections 2778, *et seq.*) "provides [to the President] the authority to control the export of defense articles and services," which authority the President delegated to the Secretary of State through Executive Order 11958.[3] The AECA is designed to "control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United Sates involved in the export and import of such articles and services." 22 U.S.C. section 2778(a)(1).

The State Department's International Traffic in Arms Regulations ("ITAR") are meant to implement the AECA by regulating various defense-related "**articles**, **services**, and related **technical data**." 22 CFR Section 121.1 (emphasis added). In turn, the items that are covered by ITAR are listed in the United States Munitions List ("USML") appearing at 22 CFR Sections 122 to 130, and items are added to and subtracted from the list over time. Generally, items on the USML are only to be made available to a "U.S. person" as defined by 22 CFR Section 120.15, even within the United States.

Companies involved in the "business of manufacturing, exporting, or importing" products or services on the USML must register with the Directorate of Defense Trade Controls. 22 U.S.C. section 2778(b). These companies employ attorneys and/or specialists who work to ensure compliance with applicable laws and regulations. In the past, there has been little need for ordinary Americans to be concerned with the AECA or ITAR, aside from restrictions on physically taking certain items to other countries. The Proposed Regs, however, would appear to change all this; indeed, it seems that the sweep of these highly technical ITAR would be broadened in ways that would regulate innumerable gun owners never before covered by ITAR.

There are numerous problems associated with the proposed expansion of the scope of ITAR. First, the AECA was never designed to apply to the activities of the average American gun owner, yet the Proposed Regs would appear designed to change this, without statutory authorization.

Second, the average American gun owner could never hope to understand or comply with the highly technical ITAR. Even lawyers, and others with the requisite technical background in this area, find ITAR daunting. Normal people, though, will have no idea which activities are covered by the Proposed Regs and which are not, and which regulations apply to them, and which do not.

Third, the Proposed Regs apply to ordinary people doing ordinary things, and this is of great concern, as there is significant confusing and ambiguous language that encompasses

---

[3] https://www.pmddtc.state.gov/regulations_laws/aeca.html.

verbal or written communications related to firearms. American gun owners must not be subject to the whim of government officials who choose how to interpret vague terms and definitions, and who may have political motivations to impose penalties for behavior that they unilaterally determine to be criminal. As such, the Proposed Regs present a serious "Due Process" constitutional concern.

Fourth, the Proposed Regs chill the exercise of legitimate First Amendment speech relating to firearms, as well as the lawful exercise of Second Amendment rights — a "double whammy" abridging both First Amendment speech and Second Amendment activities.

Fifth, the Proposed Regs would divert federal employees from focusing on matters that are in the national interest — such as maintaining confidential information about nuclear weapons or strategic bombers — and have them instead mistakenly focusing on regulating basic information about firearms — an invention that originated in China in the 12th Century, and which has been changed and enhanced, probably, in every country of the world since then.

Sixth, the Proposed Regs are represented to be a component of the "President's Export Control Initiative," which President Obama said is designed "to bring transparency and coherence to a field of regulation which has long been lacking both."[4] Unfortunately, the Proposed Regs would have the exact opposite effect, both confusing and obscuring the scope and effect of ITAR.

For these reasons, the Proposed Regs should be withdrawn, in toto.

2. Key Provisions in Proposed Regulations

Buried within the Proposed Regs' definitional changes are various small modifications to current law. When the interplay between these several sections is pieced together into the larger puzzle, a very disturbing picture appears.

a. Vast Expansion of "Technical Data"

The Proposed Regs claim to "propose[] to revise the definition of 'technical data' … in order to **update and clarify** the scope of information that may be captured within the definition." 80 Fed. Reg. 31526 (emphasis added). In reality, the Proposed Regs would bring about a **vast expansion** of what constitutes "technical data." Currently, the term "technical data" is defined as including "information" such as:

---

[4] http://export.gov/ecr/index.asp

- "blueprints"
- "drawings"
- "photographs"
- "plans"
- "instructions"
- "documentation"

The Proposed Regs seek to add to that definition the following:

- "written or oral communications"
- "diagrams" and "models"
- "formulae"
- "tables"
- "engineering designs and specifications"
- "computer-aided design files"
- "manuals or documentation"
- "electronic media"
- "information gleaned through visual inspection"

The Proposed Regs claim that "this is not a change in the scope of the definition," but simply an attempt to "harmonize" ITAR with other sections of federal law. Yet in the next breath the Proposed Regs claim to "set forth a broader range of examples of formats that 'technical data' may take." Although the State Department might attempt to justify such a broad sweep by promising to exercise enforcement discretion, the Proposed Regs would appear to have a unusually broad application to a wide assortment of constitutionally protected activities. For example:

- Presumably, all emails, text messages, phone calls between and among firearms owners relating to firearms technology, as well as all Internet posts, would fall under "written or oral communications."
- Presumably, "diagrams" would involve firearm disassembly and assembly instructions.
- Presumably, "formulae" would involve firearm ammunition loading information.
- Presumably "tables" would include ballistic tables of ammunition performance.
- And presumably "engineering designs and specifications" and "computer-aided design files" would include such things as firearm blueprints designed for 3D printing.

All of these sorts of information are items that currently are widely shared by millions of firearm owners on a daily basis across the country. For the State Department to suddenly claim that such innocuous protected Second Amendment activities are now subject to ITAR is beyond the pale. To be sure, ITAR currently does not impose restrictions on sharing

information that is in the "public domain." However, as seen below, that too would change under the Proposed Regs.

b. Severe Curtailment of the "Public Domain."

Currently, the definition of "technical data" does not include "information in the public domain." 22 CFR Section 120.10(a)(5). "Public domain" includes "information which is published and which is generally accessible or available to the public." 22 CFR Section 120.11(a). The Proposed Regs appear to radically alter that exemption.

No longer would dissemination be permissible so long as the information is "generally accessible or available to the public." Instead, and in addition, it would be necessary under the Proposed Regs first to ensure that the original publication was lawful. Indeed, the Proposed Regs claim that since "'technical data' may not be made available to the public without authorization," any "further dissemination of 'technical data' or software that was made available to the public without authorization is a violation of the ITAR." *Id.* at 31528.

To be sure, the Proposed Regs would require "knowledge that [it] was made publicly available without" authorization. *Id.* But what sort of "knowledge" is required? Actual knowledge? Constructive knowledge, where it is assumed the person knows or should know? This is the problem when unelected bureaucrats draft imprecise regulatory language which appears to create new federal offenses.

Writing about the abuses that can flow from an Independent Counsel, Seventh Circuit Senior Judge Richard A. Posner made important comments on such criminal laws:

> The machinery of federal criminal investigation and prosecution, with its grand juries, wiretaps, DNA tests, bulldog prosecutors, pretrial detention, broad definition of conspiracy, heavy sentences (the threat of which can be and is used to turn criminals into informants against their accomplices), and army of FBI agents, is very powerful; there is a fear that fed enough time and money, it can nail anybody. There is some truth to this, since there are literally **thousands of federal criminal laws, many of them at once broad, vague, obscure, and underenforced**.... [R. Posner, An Affair of State, Harvard University Press, p. 87 (1999) (emphasis added).]

It should be the duty of a federal official to ensure that regulations implementing federal laws are not "broad, vague, [and] obscure…."[5]

Because of the patent ambiguity of this section of the Proposed Regs, the new requirement would place a great burden on the American public by requiring ordinary people to determine the original legality of publicly available information. For example, a person could not even talk to his neighbor about an article in a firearm magazine without first running down the sources for the original article to make sure their release was authorized.

While the regulations do not expressly state such a motivation, this particular new requirement could provide the Obama Administration with a backdoor to go after those Americans who downloaded Cody Williams' computer model for his 3D printed firearm, which the federal government has claimed is an ITAR-regulated item, ordering Williams to stop sharing his creation.[6] It appears the Proposed Regs could be used to make criminals out of anyone who continues to use or share such information, which is nothing more than information about how to make an unsophisticated firearm for one's own use at home — generally a lawful endeavor. The Proposed Regs could also be used to provide a basis to criminally prosecute behavior which was lawful when undertaken, having the effect of creating an unconstitutional *ex post facto* law.

c. Release of "Encryption" Information

The Proposed Regs claim that the overseas transmission or storage of "technical data" is permissible so long as it is encrypted. 80 Fed. Reg. 31527. However, the Proposed Regs purport to add a new type of "release" of technical data for "any disclosure of these decryption keys or passwords." *Id*. The release of such decryption information would be considered the same as the release of the technical data itself.

There are numerous problems associated with this aspect of the Proposed Regs. First, the Proposed Regs prohibit "any disclosure" — apparently even accidental or unknowing disclosure. It has been said that ITAR are based on the assumption of "strict liability," without any requirement of scienter.[7]

---

[5] Even God did not judge before the law had been clearly declared; neither should the state. "For until the law sin was in the world: but sin is not imputed when there is no law." Romans 5:13.

[6] https://www.youtube.com/watch?v=H9MsYlnJVkM

[7] "Intent is not a requirement for an ITAR violation to be assessed. Strict liability is the standard for anyone, anywhere, who falls under the ITAR's jurisdiction. The penalties may include a $1 million fine (per violation), up to 10 years in prison…." Z. Hadzismajlovic,

Second, the Proposed Regs require only that the disclosure "may result in … unauthorized disclosure" — it is not necessary that any such disclosure actually occur for the imposition of criminal sanctions.

Third, the Proposed Regs apparently do not require that the person disclosing the information even have knowledge that his actions could lead to disclosure of technical data. Other sections of the Proposed Regs require an act be "done with the knowledge" that it is unlawful and may lead to unauthorized dissemination. *Id.* at 31528. Even someone who innocently gave decryption information for a large collection of data without knowing that some of the data were ITAR "technical data" could be at risk of prosecution.

d. Crackdown on Internet Communications

The Proposed Regs state that "before posting information to the Internet, you should determine whether the information is 'technical data.'" *Id.* at 31529. Thus, the Proposed Regs purport to create a new duty on every American to verify that innocuous Internet posts and communications do not inadvertently fall within the broad scope of what State considers to be "technical data." In practical terms, this means that an ordinary American gun owner would be required to hire a lawyer to wade through a multitude of federal regulations before he could do such simple things as make a post on a gun forum about a new "loading" he worked up for a popular hunting cartridge, or before he could send an email to a friend about what size bit to use to drill out the trigger pin hole on an 80 percent AR-15 receiver ("written communications" about the "manufacture" of "a defense article").[8] Arguably information about 80 percent receivers is already in the "public domain" but, of course, one would have to wonder whether that information was ever properly released, based on the Proposed Regs' elimination of that safe harbor.

The Proposed Regs then go further, giving a stern warning to anyone who uses the Internet or email that they will be held accountable for matters entirely outside of their control — in view of the fact that information on the Internet is routed by international telecommunication companies:

> ITAR-controlled "technical data" may be electronically routed through foreign servers unbeknownst to the original sender. This presents a risk of unauthorized access and creates a potential for inadvertent ITAR violations. … Any access to this data by

---

"Foreign Nationals and Defense Hiring: The Most Delicate of Decisions," New York Law Journal, August 6, 2012, http://goo.gl/GqszgI.

[8] http://cdn.shopify.com/s/files/1/0218/5770/files/Jig_Manual_80_Percent_Arms.pdf?106

> foreign person would constitute an unauthorized "export" under ITAR.... [at 31529]

3. Conclusion.

The State Department already has demonstrated that it can abuse its ITAR authority, and certainly should not be entrusted with more arbitrary enforcement power. By way of illustration, in 1994 the federal government pursued a criminal investigation against Phillip Zimmerman for sharing his computer software designed to encrypt data. The government claimed he had been exporting "dangerous munitions."[9] After a two-year battle, the federal investigation was finally dropped.[10]

In 2003, federal prosecutors unsuccessfully prosecuted Alex Latifi for sending a schematic diagram of the Blackhawk helicopter to a Chinese corporation, hoping that company could manufacture a part for the aircraft. The drawing he was accused of sending was already widely available on the Internet, and the Blackhawk helicopter was no secret to the Chinese, whose government already owned numerous models. Nevertheless, in its overzealousness to somehow "keep[] sensitive U.S. military technology from falling into the wrong hands," the United States government destroyed Latifi's business and the jobs of his 60 employees, bankrupted him personally, and ruined years of his life.[11]

In 2013, the State Department went after Cody Wilson, a student at the time, for his work with respect to a creative new way to manufacture firearms through 3d printing.[12] The State Department claimed that — by sharing with Americans the technology to help them build their own firearm, something clearly protected by the Second Amendment — Wilson was manufacturing and exporting "defense articles" without an ITAR license or permission to share his work. The matter apparently is still pending. As discussed above, the Proposed Regs seem to be particularly designed to give the State Department more authority over this sort of Second Amendment activity.

---

[9] http://readingroom.law.gsu.edu/cgi/viewcontent.cgi?article=2264&context=gsulr.

[10] http://www.skypoint.com/members/gimonca/philzim2.html.

[11] *See, e.g.,* S. Horton, "Another Abusive Prosecution by Alice Martin," Feb. 24, 2008 http://harpers.org/blog/2008/02/another-abusive-prosecution-by-alice-martin/; D. Lynch, "Feds knock; a business is lost," USA Today, July 10, 2008 http://usatoday30.usatoday.com/money/smallbusiness/2008-07-09-axion-blackhawk-latifi-martin_N.htm

[12] http://reason.com/blog/2015/05/11/cody-wilson

The Proposed Regs are ambiguous and confusing. The Proposed Regs violate the First, Second, and Fifth Amendments. American gun owners need to be reassured that they will remain free to engage in innocuous activities such as posting ammunition ballistics on a blog, or emailing a manufacturer asking about the battery life of a red dot optic they are looking to purchase. Under the Proposed Regs, American gun owners could be subject to prosecution for engaging in such innocent activity. For all the reasons stated above, the Proposed Regs must be withdrawn.

Sincerely yours,

/s/

Robert J. Olson

RJO:ls