THE LINUX FOUNDATION

Understanding Open Source Technology & US Export Controls

了解开源科技和美国出口管制

Open development enables global collaboration: a guide for companies using and developing open source technology

开源发展使全球协作成为可能: 一份致使用与开发开源科技公司的指南

A Publication of The Linux Foundation | July 2020; updated July 2021

Linux基金会出版物 | 2020年7月, 于2021年7月七月

One of the greatest strengths of open source development is how it enables collaboration across boundaries. Open source collaboration occurs transparently, publicly, and across organizational boundaries: individual developers, academics, and employees across the globe can come together and build an open technology that is greater than any of them could individually produce.

Open source collaboration also occurs across geographic boundaries: people and organizations from a multitude of countries around the world bring their unique perspectives and strengths to build together in the open, and to release the results to all.

Because open source development is a global activity, it necessarily involves making available software across national boundaries. Some countries' export control regulations may require taking additional steps to ensure that an open source project is satisfying obligations under local laws. This article briefly describes the Export Administration Regulations of the United States and discusses how they apply to open source communities developing technology in global collaboration. In this article, we will generically refer to "open source" as any technology or software where the source is made publicly available. Open source as a creation model has evolved to cover more than just software technology. Open source now includes a wide range of open technology segments such as hardware designs, microprocessor instruction set architectures, specifications, data models, protocols, standards and any other technology that groups are collaborating to build publicly, in the open.

开源发展的最大优势之一是它实现了跨边界的协作。开源协作透明、公开且能跨越组织边界，促使世界各地的开发人员、学者和工作人员一同成就比个人力量所能造就的更为伟大的开源技术。

开源协作跨越地域界限：聚集世界各国人员和组织,带着他们独特的观点和优势来一同开放协作，并向所有人分享成果。

开源发展是一项全球性活动，必然涉及软件的跨国界分享。一些国家的出口管制法规可能要求开源项目采取额外的措施，来确保遵守当地法律规定的义务。这篇指南将简要地描述美国《出口管制条例》，并讨论该条例如何应用于开源社区发展全球协作。本文中，“开源”一般指的是任何源码可公开获取的技术或软件。作为一种创造模式，开源已不仅仅局限于软件技术的开发。如今，开源还包括了其他广泛的开放技术领域，如硬件设计、微型处理器指令集架构、规范、数据模型、协议、标准以及公众以公开模式协作创造的其他技术。

The US Export Administration Regulations

The primary source of United States federal government restrictions on exports are the Export Administration Regulations, or EAR. The EAR is published and updated regularly by the Bureau of Industry and Security (BIS) within the US Department of Commerce.[1] The EAR applies to all items "subject to the EAR," and may control the export, re-export or transfer (in-country) of such items.

Under the EAR, "export" has a broad meaning. Exports can include not only the transfer of a physical product from inside the US to an external location, but also other actions. For example, releasing technology to someone other than a US citizen or lawful permanent resident within the United States is deemed to be an export,[2] as is making available software for electronic transmission that can be received by individuals outside the US.

At first this may seem alarming for open source communities, but the good news is open source technologies that are published and made publicly available to the world are not ordinarily subject to the EAR. Therefore, open source remains one of the most accessible models for global collaboration.

In the following sections, we will explain why concerns over the United States export control regulations are generally not a problem for the open source model and discuss how the EAR generally does not apply to the export of open source software with a few example situations. We will then address two subject matter areas in certain circumstances: first, open source software that includes non-standard cryptography functionality; and second, open source software that implements neural network-driven geospatial analysis training functionality. Finally, we will suggest some best practices for open source communities to consider in their projects.

美国的《出口管制条例》

《出口管理条例》(Export Administration Regulations, 以下简称"EAR") 是美国联邦政府限制出口的主要条例, 由美国商务部 (US Department of Commerce) 下的产业与安全局 (Bureau of Industry and Security, 以下简称"BIS") 发布并定期修订。[1] EAR适用于所有"受制于EAR"的物品, 并可能管制该等物品的出口、再出口或 (境内) 转让。

EAR下"出口"的定义较为宽泛。出口不仅包括从美国境内向境外输送实物产品, 还包括其他行为, 例如向非美国公民或非美国合法永久居民传送技术, [2] 以及向美国境外人员提供用于电子传输的软件。

从表面看来, EAR似乎为开源社区敲响了警钟, 但是好消息是， 公开发布给全世界享用的开源技术通常是不受制于EAR的。因此， 开源至今仍然是一个最为便利的全球协作的模式

在接下来的内容中, 我们将解析为 何美国的出口管制法规一般不会对开源模式造成影响, 并通过举例的方式说明和讨论为何开源软件的出口在一般情况下不受制于EAR。 接着 , 我们将探讨在 一定情况下的两个特定事项的范围: 第一, 包含非标准加密功能的开源软件; 第二, 实施由神经网络驱动的地理空间分析训练 (neural network–driven geospatial analysis training) 功能的开源软件。最后, 我们会提出一些最佳实践建议, 供开源社区在项目实施过程中采纳。

1 Currently available at / 请见 **https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear**

2 See § 730.5(c), currently available at / 见第730.5(c) 部分 **https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.730_15&rgn=div8**; see definition of "foreign person" in § 772.1, currently available at / 见第 772.1部分对"外国人"的定义 **https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.772_11&rgn=div8**

Applying the EAR to Open Source Software

The EAR defines the scope of certain items, including software and technology, that may be subject to export restrictions. The EAR provides for Export Control Classification Numbers, or "ECCNs," for different types of items, including software and technology. Some items are subject to the EAR, meaning that they are inside the EAR's scope and may only be exported if: the EAR permits the export without a license, a license exception applies, or a license to export is obtained.

This is where open source technologies are advantageous because the EAR explicitly exempts most software and technology made available as open source. Some items are specifically not "subject to" the EAR at all, meaning that they are *"outside the regulatory jurisdiction of the EAR and are not affected by these regulations."*[3] Specifically, the EAR states in § 734.3(b)[4], *"The following are not subject to the EAR:"* and then lists, *"Information and 'software' that: (i) Are published, as described in § 734.7".* The reference to § 734.7 is important as this section states materials that are "published" are not subject to the EAR. Specifically, the EAR § 734.7 states[5],

> *... unclassified "technology" or "software" is "published," and is thus not "technology" or "software" subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination...*

Open source software from the Linux Foundation and project communities we work with is "published" as described in EAR § 734.7.

将EAR应用于开源软件

EAR界定了某些可能受到出口限制的事项 (包括软件和技术) 的范围。"ECCNs" (Export Control Classification Numbers) 是EAR法下用于不同种类物品 (包括软件和技术) 的编码。有些物品是受制于EAR的， 这代表它们在EAR的管控范围内, 并只能在符合以下条件的前提下出口： 无需许可证就可出口, 适用许可证 例外的情况或者出口方已经获得了出口许可证。

这正是开源技术的优势所在, 因为EAR明确豁免了大多数以开源形式呈现的软件和技术。有一些事项被明确列为"不受制于"EAR, 意味着它们"被置于EAR法规管辖外并不受这些法规的 约束 。"[3] 具体来说, EAR第734.3 (b) [4] 条规定"下列事项不受制于EAR: ", 其后列明, "如第734.7 条所述的, (i) 已经发布的信息及'软件'"。 这里指向第734.7条是非常重要的 , 因为该部分规定"已发布"的事项不受到EAR的管辖。具体来说, EAR第734.7部分规定5,

> . . .当可被公众获取且无进一步传播限制时, 未被归类为密级事项的"技术"或"软件"属于" 已发布", 因此不属于受EAR管辖的"技术"或"软件" . .

来自Linux基金会以及与我们合作的项目社区的开源软件均 满足EAR第734.7条中"已发布"的要求。

3 See § 734.2(a)(1), currently available at / 请见第734.2(a)(1)部分，现可在 **https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.2.734&rgn=div5#se15.2.734_12** 获取

4 See § 734.3(b), currently available at / 请见第734.3(b)部分，现可在 **https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.2.734&rgn=div5#se15.2.734_13** 获取

5 See § 734.7, currently available at / 请见第734.7部分，现可在 **https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.2.734&rgn=div5#se15.2.734_17** 获取

The following typical scenarios (but not an exhaustive list) are not subject to the EAR because "open source" is "published":

- Open source software that is published publicly is not subject to the EAR
- Open source specifications that are published publicly are not subject to the EAR
- Open source files that describe the designs for hardware that are published publicly are not subject to the EAR
- Open source software binaries that are published publicly are not subject to the EAR

The key word is the word "published." For the purposes of the EAR, if the open source technology is publicly available without restrictions upon its further dissemination, then it is "published" and therefore "not subject to" the EAR. It would be a major shift in existing policy for the EAR to be changed to make "published" software and technology subject to EAR restrictions, and we are not aware of any current discussion for such a change.

The US position that publicly available software or technology is not subject to export control is also not specific to the US regulations, but also includes the European Union.

Additionally, activities that do not relate to software, technology or other items within the EAR's scope are not subject to the EAR. Non-technical collaboration falls into this category: meetings about business matters, event planning, marketing, and similar activities are not subject to the EAR, because they are outside its scope.

To meet the requirement of "published" under the EAR, open source communities may need to take one additional step if the project includes non-standard cryptography technology.

以下典型事项 (未详尽列举) 下不受到EAR限制, 因为"开源""已发布":

- 已公开发布的开源软件不受制于EAR
- 已公开发布的开源规格不受制于EAR
- 已公开发布的, 说明硬件设计的开源文档不受制于EAR
- 已公开发布的开源软件二进制不受制于EAR

如此可见, "已发布"是关键要素。基于EAR之目的, 如果开源技术不受进一步传播的限制且可被公开获取, 那么它将被视为"已发布"了的开源事项, 并将因此"不受制于"EAR。将"已发布"的软件和技术纳入受制于EAR限制的范围内将是一项重大的政策性转变, 迄今为止我们尚未知悉任何关于上述政策性转变的讨论。

可公开获取的软件和技术不受制于出口管制并非美国独有的政策, 欧盟也有相关政策。

另外, 与软件、技术和其他在EAR范围内的事项无关的活动也不受EAR限制, 其中包括非技术性协作: 有关商务事项的会议、活动策划、市场营销等类似的其他活动均不受EAR约束, 因为上述事宜超出了EAR管辖范围。

若项目涉及非标准加密技术, 则开源社区可能需要多采取其他措施以满足EAR法下的"已发布"的要求。

Encryption Implementing Non-Standard Cryptography

The EAR used to require an email notification for any many types of encryption technology published as part of an open source project. This requirement was changed in 2021. The email notification requirement now applies only to publicly available encryption software that implements a "non-standard cryptography".[6] "Non-standard cryptography" is defined by the EAR as "any implementation of 'cryptography' involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA) and have not otherwise been published."[7]

Among other subject areas, software developers focus on encryption, which is of primary importance in the EAR. The EAR regulates exports of certain encryption software and technology. The definition of "encryption software" is very broad and can include software that merely activates or enables encryption features in another software or hardware product.[8] For software implementations of standard encryption functionality, including encryption hardware when represented in software design files, the most common ECCN classification is 5D002. If encryption software is "subject to" the EAR, then in order to export it anywhere except to Canada, one would need to first confirm that an exception applies, or request and obtain a license from BIS to permit the export.

However, before considering whether an exception or export license is necessary, the first question should be: is the encryption software "subject to" the EAR at all?

实施非标准加密技术进行加密

对于作为开源项目一部分发布的多种类型的加密技术，EAR过去都要求发送电子邮件通知。这一要求在2021年发生了变化。有关电子邮件通知的要求现在仅适用于实施"非标准加密"技术的可公开获取的加密软件。[6] 根据EAR的定义，"非标准加密"是指"结合或使用专有或未公布的加密功能实施'加密'，包括尚未被正式认可的国际标准机构（如IEEE、IETF、ISO、ITU、ETSI、3GPP、TIA和GSMA）采用或批准的，以及尚未公布的加密算法或协议。"[7]

除其他事项外，软件开发者的关注焦点便是加密技术，这是EAR中最重要的内容。EAR 管理特定加密软件和技术的出口。"加密软件"的定义非常广泛，并可能包括仅激活或创设其他软硬件产品的加密功能的软件。[8] 对于具备标准加密功能的软件，包括在软件设计文档中呈现的加密硬件，最为常见的ECCN类别是5D002 。如加密软件在EAR的管辖范围内，那么为了将其出口到除了加拿大以外的国家，出口方必须首先确认EAR例外条款在此情况下适用，或申请并从BIS获取相应的出口许可证。

然而，在考虑EAR例外条款是否适用或出口许可证是否必要前，首先要考虑的问题是：该加密软件是否在EAR 的管辖范围内。

6 See **https://www.federalregister.gov/d/2021-05481/p-47**

7 See "non-standard cryptography" at **https://ecfr.io/Title-15/Section-772.1**

8 See §772.1, currently available at / 请见第772.1部分，详情请见 **https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.2.772&rgn=div5** 获取

Encryption source code classified under ECCN 5D002 is not subject to the EAR if both (1) it is "publicly available," and (2) either implements a standard, publicly available cryptography, or implements a non-standard cryptography and an email notification has been sent for it to the addresses listed in that section .[9]

For the first part of the test, the meaning of "publicly available" refers to the EAR's definition of "published," which includes public dissemination by posting on the Internet on sites available to the public.[10] Given this, the first part of the test should be met for all fully-public open source software projects: if the project's source code is openly available on the Internet, then it should be considered "publicly available."

The second part of the test requires a determination of whether the publicly available encryption technology implements non-standard cryptography. Implementing non-standard cryptography, will require that an email be sent to two specified email addresses, one at BIS and the other at the US National Security Agency (NSA). The email should include the URL of the publicly available code (or a copy of the code itself). An updated notification should be sent later if the previously provided URL or copy has changed.[11]

Finally, after the two-part test is satisfied, then its corresponding object code counterpart is also not subject to the EAR.[12]

It is rare to find non-standard cryptography in an open source software project. Anyone using such a form of cryptography should consult a legal advisor on how to proceed.

属于ECCN 5D002的加密源代码如符合以下两个条件，则不在EAR的管辖范围内：（1）该源代码是"可公开获取"的，以及(2)实施一种标准的、公开可获得的加密技术，或实施一种非标准的加密技术 并向该部分中已列出的地址发送电子邮件通知。[9]

上述衡量标准的第一部分要求，即"可公开获取"，指的是在EAR法下"已发布"的定义，这包括通过在公开的网页上进行发表（即公开传播）。[10] 只要完全公开的开源软件项目达到该标准，则应当视为通过了衡量标准的第一部分要求：如果项目的源代码可在互联网上公开获取，则应被视为"可公开获取"。

上述衡量标准的第二部分要求确定可公开获取的加密技术是否实施了非标准加密技术。实施非标准加密技术将需要向两个指定的邮箱地址发送邮件（一个是BIS的邮箱地址，另外一个是国家安全局（National Security Agency，简称"NSA"）的邮箱地址）。邮件内容需要包括可公开获取的源代码的URL地址（或源代码本身）。如URL或源代码发生任何变更，则需要再次以邮件形式通知上述邮箱地址。[11]

最后，在通过了上述两项衡量标准后，相应的目标代码也将不受EAR管辖。[12]

在一个开源软件项目中发现非标准加密是非常罕见的。任何使用这种加密形式的人都应咨询法律顾问具体应如何进行。

9 See §742.15(b), currently available at / 请见第742.15（b）部分，详情请见 **https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.742_115&rgn=div8**

10 See §734.7, currently available at / 请见第734.7部分，现可在 **https://www.ecfr.gov/cgi-bin/retrieveECFR?n=pt15.2.734&r=PART&ty=HTML#se15.2.734_17** 获取; §734.3(b)(3), currently available at / 第734.3(b)(3)部分，现可在 **https://www.ecfr.gov/cgi-bin/retrieveECFR?n=pt15.2.734&r=PART&ty=HTML#se15.2.734_13** 获取

11 See § 742.15(b), currently available at / 请见第742.15（b）部分，现可在**https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.742_115&rgn=div8** 获取

12 See / 请见 **https://www.bis.doc.gov/index.php/policy-guidance/encryption/223-new-encryption**

At The Linux Foundation, the source code for all of our projects, including encryption software, is publicly available. In most if not all cases, it is standard cryptography, and we have additionally provided email notices as described above for many of our projects. We also make copies of these email notices publicly available for viewing on the LF's website.[13] As a result, the Linux Foundation's project source code and corresponding object code are not subject to EAR encryption restrictions.

Please keep in mind that this applies only to the open source project itself. Downstream redistributors of modified project code, or products derived from it, where the source code is not publicly available would still need to evaluate their own compliance with the EAR (just as with any other software that they export).

Linux基金会的所有项目源代码, 包括加密软件, 均可公开获取。在绝大多数情况下, 这些源代码都是标准加密的, 并且我们在许多项目中还另外提供了 上文所要求的电子邮件通知。 并在我们的官网上公开了上述电子邮件通知的 内容。[13] 所以, Linux 基金会的项目源代码及对应的目标代码均不受 EAR 关于加密的限制。

请注意, 上述情况只适用于开源项目本身。修改项目代码或其衍生产品的下游再分销商在源码并未公开时, 仍然需要评估其是否符合EAR的规定（ 如同需评估其出口的其他软件一样）。

13 **https://www.linuxfoundation.org/export/**

Neural network-driven geospatial analysis training

On January 6, 2020, BIS announced a new EAR rule that immediately went into effect. This rule established EAR controls over a specific kind of geospatial imagery software that is specially designed for training a Deep Convolutional Neural Network[14] to automate the analysis of geospatial imagery and point clouds. The rule clarifies that a "point cloud" refers to a collection of data points defined by a given coordinate system, also known as a digital surface model.[15] Although the rule went into effect immediately upon publication, it remains subject to comment and may continue to develop or change. In any case, if it is publicly available software (e.g. open source software) then it still would not be subject to the EAR, as described above.

Some public portrayals of the new rule may have implied that it imposed broad prohibitions on geospatial imagery software, or even on artificial intelligence / machine learning software as a whole. That is not the case.

The scope of the rule actually appears to be quite narrowly tailored. It applies only to that which specifically includes all of the aspects described above. Furthermore, in order to be subject to the new EAR rule, the software must also include all of the following functionality:

1. Provides a graphical user interface that enables the user to identify objects (e.g., vehicles, houses, etc.) from within geospatial imagery and point clouds in order to extract positive and negative samples of an object of interest;

神经网络驱动的地理空间分析训练

BIS在2020年1月6日宣布了一项新的EAR规定，并自宣布之日起立即生效。该规定设立了EAR针对一种专门为了训练深度卷积神经网络[14] (Deep Convolutional Neural Network) 自动分析地理空间图像和点云 (point cloud) 能力的特殊地理空间图像软件的管控权。该规定阐明"点云"是指由坐标系统界定的数据点集合，又称数码表面模型。[15] 虽然规定自发布之日立即生效，但它仍有待 公开意见征求并可能继续扩充或被修订。但无论如何，如果软件是可公开获取的 (如开源软件)，那么如上文所述，它将不受 EAR的管辖。

一些对新规定的公开解读可能在暗示该规定整体上对地理空间图像软件，或甚至人工智能/机器学习软件施加了广泛的限制。但事实并非如此。

这条规定的适用范围实际上显得很狭窄。它只适用于具体包括上述所有方面的事项。此外，　任何一项软件同时还必须包括以下所有功能，才受 这条新EAR规定的 管辖:

1. 提供图形用户界面，使用户能够从地理空间图像和点云中识别物体 (例如，车辆、房屋等)，以便提取物体的阳性和阴性样本 (positive and negative samples)；

14 Although "Deep Convolutional Neural Network" is not defined in the regulation, for background information see, e.g., / 虽然法规未界定"深度卷积神经网络"，请参下列背景材料，如，**https://en.wikipedia.org/wiki/Convolutional_neural_network; https://wiki.pathmind.com/convolutional-network**

15 See 85 FR 459, currently available at / 请见85 FR 459，请见 **https://www.federalregister.gov/d/2019-27649/p-12**

2. Reduces pixel variation by performing scale, color, and rotational normalization on the positive samples;

3. Trains a Deep Convolutional Neural Network to detect the object of interest from the positive and negative samples; and

4. Identifies objects in geospatial imagery using the trained Deep Convolutional Neural Network by matching the rotational pattern from the positive samples with the rotational pattern of objects in the geospatial imagery.

If software does not include every one of the aspects and functionality listed above, then it appears that it would not be subject to the new restrictions in their current form. The list of requirements reads very closely to what you might expect a commercial solution provider to deliver as a solution, not as an open source project. In particular the requirement for training would require not only a software project but a training dataset of positive and negative samples that would likely only apply to a specific implementation of the neural network.

There may be some publicly available, open source projects today that implement this functionality. However, even if a new project were to be created today, as long as it is run as a publicly available open source project then it would not be subject to the EAR.

2. 通过对阳性样本进行尺度、颜色和旋转归一化来减少像素变化范围；

3. 训练深度卷积神经网络从阳性样本和阴性样本中探测到物体；和

4. 利用训练好的深度卷积神经网络，将阳性样本的旋转模式与地理空间图像中物体的旋转模式进行匹配进而识别地理空间图像中的物体。

如软件不具备上述列出的所有方面和功能，那么该软件则似乎不受 该条新规定（目前版本）的管辖。上述要求更像 是针对由商业解决方案提供商提供的解决方案，而不是 针对开源项目。特别是，训练要求不仅需要一个软件项目，并且还需要阳性和阴性的训练数据集，这种对数据集的具体要求可能只适用实施特定的神经网络。

现有的一些可公开获取的开源项目可能具备这些功能。然而，即使现在要创建一个新的项目，只要该项目是一个可公开获取的开源项目，那么它就不会受 EAR的管辖。

Best Practices for Open Source Software Communities

There are a few practices we have learned or developed that may be helpful for all open source communities.

Be Open and Be Public

We often use the word “open” to mean many things: an open source license, open and transparent discussions, open community, openly available source code on a public repository. “Open” may seem an obvious practice for open source communities, but there are some recommendations for communities.

First, communities should strive to keep their technical conversations open and public. If private conversations happen within communities, that’s normal, it is recommended to make the community decisions and outcomes publicly available. It is important for our projects to make information available transparently and publicly as the private exchange of technology or technical information may not meet the “publicly available” standard according to the EAR.

One question that has come up has to do with exchanges of information related to security issues under a security disclosure process. As a best practice, projects may want to consider making exchanges like this public upon availability of fixes, and not limit this information to only the confidential disclosure list.

Exchanging technical ideas and knowledge, and having a technical debate are hallmarks of open source communities where the best technical solutions

开源软件社区的最佳实践

以下是一些我们了解到或者尝试过的可能对所有开源社区有所助益的一些实践经验。

公开化和公众化

我们经常用“公开”这个词来形容许多事情: 开源许可、公开和透明的讨论、公开的社区、公共智库里储存的可公开获取的源代码。对于开源社区来说, “公开”似乎是显而易见的做法, 但我们对社区也提供一些建议。

首先, 社区需要努力 维持他们技术交流的开放性与公开性。私人交流在社区中经常出现 , 对此我们建议将社区决策和结果向公众公开。信息的公开透明对我们项目来说很重要, 因为技术或技术信息的私下交换可能不符合EAR中“可公开获取”的标准。

安全系统缺陷披露的过程中涉及到的信息交换会引起问题。对此, 我们建议最好可在缺陷修复后公开项目交流内容, 而不仅限于 向保密披露清单里的各方提供。

should rise to the forefront. These exchanges may be uncomfortable to have in public at times, but our communities who strictly hold to this principle are often the most successful at building transparent and trusting communities. There may be disagreements, but everyone knows the discussion is happening in public and transparently - there are many positive benefits to public, open collaboration beyond just meeting requirements in the EAR.

Use standard cryptography for encryption

It is generally best to avoid non-standard cryptography that is also not publicly available for encryption in an open source project.

If your open source software project decides to provide or perform encryption functionality classified under ECCN 5D002 and implements a form of non-standard cryptography, then you will need to deliver a notification of encryption to the BIS and the NSA according to the EAR requirements. EAR § 742.15(b)(2)[16] describes these requirements:

- Send an email to **crypt@bis.doc.gov** and **enc@nsa.gov**.
- The email should contain either the URL of the publicly available encryption source code, or a copy of the source code itself. Typically we would expect that open source projects would select the first option.
- If you provided a URL to a site where you posted the source code on the Internet, you must notify by email again each time the Internet location is changed, but you are not required to notify them of updates or modifications made to the encryption source code at the previously notified location.

交流技术思想和知识，进行技术辩论是开源社区的标志，其中最前沿的是最佳的技术解决方案。在公开场合进行这些交流有时可能会让人难以接受，但是我们那些严格遵守该原则的社区往往也是在建立透明度和可信赖性方面最为成功的社区。尽管可能会有分歧，但每个人都知道这个讨论是公开和透明的。当然公开和开放协作 有很多益处，而不仅限于其能 够符合EAR的要求。

使用标准加密法加密

通常情况下，最好避免在开源项目中使用尚未能公开获取的、非标准的加密技术。

如果你的开源软件项目决定提供或执行ECCN5002项下的加密功能，并实施非标准加密，那么根据EAR的要求，你需要向BIS和NSA提供通知。EAR第742.15 (b)(2) [16] 条 列举了以下这些要求：

- 发送电邮至**crypt@bis.doc.gov**及**enc@nsa.gov**。
- 邮件应该包括含有可公开获取加密源代码的网站地址，或源代码本身。一般来说，我们预计开源项目会选择第一种方式。
- 如果 你提供的是网站地址，那么每次更换网站地址时，你都必须通过电子邮件通知他们，但是 你不需要通知他们有关源代码本身的更新或者变更。

16 See §742.15(b), currently available at / 请见第742.15 (b) 部分，在可在 **https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.742_115** 获取

- If you provided a copy of the source code, and you update or modify the source code, you must also provide additional copies to each of them each time the cryptographic functionality of the source code is updated or modified.

As you will see in the Linux Foundation's notices,[17] we suggest a few additional details as best practices:

- Make publicly available copies of the notices that were delivered to BIS and NSA, in order to increase transparency and visibility of compliance. This also helps with your community of downstream users who may wonder "do they send notices?" You can prevent concerns by making the notices themselves public.

- Include contact information and, where applicable, the name of the particular legal entity or company that is responsible for the project.

- Establish a system to ensure that you maintain evidence, for a medium- to long-term period of time, that the notification emails to BIS and NSA were in fact delivered. Relying solely on an individual's "Sent" mailbox records may not be preferable if a question arises in the future, or if that individual loses access to that Sent mailbox.

If you are unsure whether your open source software project uses encryption based on non-standard cryptography, or if you know that it might in the future, you might also consider delivering a notice out of an abundance of caution.

- 如果 你提供的是源代码副本, 那么每当加密功能 存在更新或者变更后， 你都必须把最新的源代码提供给他们。

正如Linux基金会的通知所展现， [17] 以下我们建议的其他一些最佳实践方案：

- 为了加强透明度和展现合规性，将传给BIS和NSA的通知公开化。这也有助于解决下游用户对社区是否发送了通知的疑惑。通过公开通知的方式， 你可以避免这些困扰。

- 附加联系方式和负责项目的法人实体或公司的名称（如适用）。

- 设计一个保留中期至长期证据的系统 ，以证明发送给BIS和NSA的通知电邮实际上已经送达 。 最好不要仅依靠"已发送"邮箱记录，以避免将来发生问题， 和规避该个人无法再访问该"已发送"邮箱 的风险。

如果 你不确定 你的开源软件是否使用了基于非标准加密技术的加密功能，或你知道将来可能会使用这种功能，那么为确保万无一失， 你也可以考 向相关部门发送此类通知 。

17 **https://www.linuxfoundation.org/export/**

Ensure corresponding encryption source code is publicly available

If you are distributing publicly available encryption software in object code form, then you will also want to ensure that it is publicly available in source code form as well.

Maintainers of the project, who are most familiar with the project's code, should review to see if there are instances where encryption functionality is distributed in binary or object code form. Where it is, consider first if that is necessary. Distributing in source code form may be a preferred approach—not only for export compliance purposes, but also so that downstream users are not dependent on trusting a "black box" binary, and can easily build it themselves from source code.

If it is necessary to distribute encryption software in binary or object code form, then ensure that the corresponding source code is publicly available.[18] The easiest way to do this is to make available the source code for that version of the encryption software yourself, as part of the project's own code. (In fact, depending on the applicable open source license, this may be necessary or at least useful in complying with that open source license as well!)

In addition to manual review, there are[19] some scanning tools with varying degrees of ability to scan source code and detect usage of encryption functionality. No automated scanning tool is likely to be a perfect detector of all applicable uses, but these may be helpful in identifying copies of encryption software in a large codebase.

确保相应的加密源代码是能够公开获取的

如果 你以目标代码形式公开分享加密软件，那么 你应确保该软件的源代码也是可公开获取的 。

项目的维护者，也是最熟悉项目代码的人群，应该审查并确认加密功能是否以二进制或目标代码形式分发的。如果是，那么应该先考 上述操作是否必要。在大多数情况下，以源代码形式分发可能是最佳的方案 – 不仅基于出口合规的考 ，并且此种方案有助于下游用户摈弃对"黑盒子"二进制的依赖，并且可以轻松地从源代码处自主研发。

如果必须以二进制或目标代码形式分发加密软件，那么就必须确定相应的源代码是可公开获取的。[18] 最容易的方式就是自主将该加密软件版本的源代码公开，作为项目本身的源代码。（事实上 ， 取决于适用的开源许可内容，从遵守开源许可的角度来说可能 必 须这样做，或者至少 有 所助益！）

除人工审核外，还有一些性能不等的扫描工具，[19] 可以扫描源代码并探测加密功能的应用。没有一种自动扫描工具能够完美地检测出所有的应用，但这些工具可能有助于识别大型代码库中的加密软件。

18 See / 请见 **https://www.bis.doc.gov/index.php/policy-guidance/encryption/223-new-encryption**

19 See, e.g., Fossology / 请见，如Fossology (**https://www.fossology.org/features/**, see under "Export Control Codes" / 浏览 "Export Control Codes"一栏); exportctrl from the Software Freedom Law Center / Software Freedom Law Center之出口管控 (**http://code.softwarefreedom.org/cgit/exportctrl/**)

The Linux Foundation promotes, protects and standardizes Linux by providing unified resources and services needed for open source to successfully compete with closed platforms.

To learn more about The Linux Foundation or our other initiatives please visit us at **www.linuxfoundation.org**