2861771 - Introduction to Encryption Export Controls

Welcome to the Department of Commerce Bureau of Industry and Security Export Regulations Training Webinar Series. Today's topic is an "Introduction to Encryption Export Controls." In just a moment we'll be turning you over to our presenters. If you're watching live you'll have the opportunity to ask questions directly using the "Ask a question" button just below the video window. We hope you enjoy the view overlooking Connecticut Avenue and K Streets in Washington, only a couple blocks from the White House. Again, thank you for attending. Now let's turn it over to our presenters.

The Information Technology Controls Division is pleased to present this brief webinar, with an introductions to Encryption Export Controls this afternoon. The Information Technology Controls Division consists of nine licensing officers; myself, Randy Wheeler, and I'm joined today by two other licensing officer, Anita Zinzuvadia and Aaron Amundson. We're going to very quickly run through a list of topics to familiarize you with the encryption export controls and the Export Administration Regulations.

The Information Technology Controls Division is responsible for classifying and licensing items that are listed in Categories 4, 5 Part 1, and 5 Part 2 of Commerce Control list; that is, computer, communications, and information security items. And we have found that at least 95% of our workload is concerned with encryption items that are found in Category 5 Part2 of the Commerce Control list.

Before launching into our slides, I would like to make a couple of notes. One is, again, this is a very brief webinar. We're going to run through a lot of terminology very quickly. But we hope that questions that come up, you will feel free to contact us after the webinar. We'll have our contact information at the end of the presentation, and we would be happy to talk to you and answer any further questions that you have.

Secondly, we are presenting the encryption provisions of the Export Administration Regulations as they are today, February 17th, 2016, and the regulations do change from time to time. In fact, as we speak, there is a rule making its way through to publication that will make some structural changes to Category 5 Part 2 of the Commerce Control list. We also hope that some additional provisions, encryption provisions, can be amended in the same rule. So, please, if you are looking to the encryption provisions, please make sure that you look at the current version of the Export Administration Regulations that are published on our website, as things do change.

Finally, just to note that there are a few handouts that are included in the webinar materials today. We have two charts, one on license exception ENC, and one on mass market encryption, and two lists of government end-users that I will be discussing later on in the presentation. So with that, I'd like to turn the slides over to Anita Zinzuvadia. These are the topics that we're going to touch on today very briefly, and we will start with the Category 5 Part 2 of the Commerce Control List.

Thank you, Randy. So I'm going to take a few minutes to discuss items that are subject to Category 5 Part 2. And when I start these discussions I like to kind of start off with a common base of understanding. And with that, first, I'd like to talk about some items that are not in Category 5 Part 2. First of all, encrypted data: the EAR, Export Administration Regulations, does not control encrypted data for the sake of it being encrypted. So that includes files, music, multimedia information, videos. Encrypted data is not controlled. But the hardware/software that could be used to encrypt that data could be controlled. So that's point number one there.

Compression: we do not consider compression to be cryptography. There's no means for hiding information in compression, or a secret key exchange used in compression. So, some of you may be familiar with tools like WinZip. It compresses the information using certain algorithms, but the compression itself is not considered encryption. But WinZip is a tool that we know that does encryption on top of the compression. So it could be considered an encryption item for the functionality but not the compression itself.

Next, coding techniques, we outline this in the regulations under Category 5 Part 2 that we do not control fixed coding techniques. Things like CDMA is not considered cryptography. Also, parity bits are not considered with your key length in encryption in counting your -- measuring your key length.

Other items that are not subject to Category 5 Part 2 include medical equipment. There's a statement of understanding in Supplement No. 3 to part 774, which essentially says medical equipment and those items that are designed for the medical treatment of patients, are not considered under Category 5 Part 2, so something like an EKG machine.

Note 4 to Category 5 Part 2, this was written in 2010, and it gives us what I call a primary function test. It allows us to decontrol many, many items out of Category 5 Part 2, even when they use encryption functionality.

And lastly, public available items. Randy will discuss further in the presentation a little bit more about publicly available items.

So what are encryption items? So we know that some of you are familiar with encryption, the use of symmetric and asymmetric encryption algorithms like AES, DES, Diffie Hellman, RSA. These are all encryption algorithms that are used to encrypt data, and they involve the secret key exchange to hide information. So the things that are subject to the EAR are hardware, software, and technology that make use of encryption.

So here we've got -- we could talk about Smartphones, routers, gateways, firewalls, and other network infrastructure items, network switches, telecommunications infrastructure that uses encryption. Generic computers can have encryption software loaded on them and have encryption hardware functionality, special purpose encryption chips, software that's loaded on your phone. Apps on your phone, on your smartphone can have encryption functionality. Operating systems running on your laptop or your mobile device or your tablet also have encryption functionality. And also reference here that software that makes calls to third-party encryption functionality is considered -- should be considered under encryption in that it is using -- it has encryption functionality even if it is not native to the code that is written. If it's calling or making a third party functional call to an encryption library, it can also be considered an encryption item.

So we also cover encryption technology, so that's, as defined in the regulations, production, development, and use technology for encryption items. So what are the ECCNs that we're talking about here? These are the commodity classification numbers under Category 5 Part 2 that apply to encryption item. We have the 002 controls. These are multilaterally agreed on by the Wassenaar Arrangement member countries. The 002 controls have a national security control and an AT control, antiterrorism control. So here we have A for hardware, D for software, E for technology, and B for testing.

Also, we have some of the low-level encryption items, so those are the 992 controls, where the AT control, the antiterrorism control, only applies. And encryption items could fall to EAR99 as well. Even items with encryption functionality do not necessarily have to be controlled under Category 5 Part 2, which I'm going to talk more about.

Another ECCN that is not actually up on the slide but worth mentioning is 5A980. That's surreptitious listening items. They're not necessarily controlled for the encryption functionality; rather, they're controlled because they're primarily useful for eavesdropping or wiretap tools, which you can get to the content of communications. And those are very restricted and in most cases, require licenses to anywhere they're going.

So this next slide is giving kind of a lay of the land in Category 5 Part 2, and what's not in Category 5 Part 2. And I like to say that the 002 control, that box at the bottom, it's like a party you don't want to be invited to, so I'm going to talk about exit strategies before we get to the 002 controls. So, hopefully, when you analyze any one of your products to try to take advantage of or use the controls that are actually used to decontrol your item outside of 002.

So I had touched already on some of the items that are not in Category 5 Part 2, the medical equipment and the publicly available, which Randy will talk about more later in the presentation. I will talk a little bit more about the primary function test that we talked about, and that I mentioned, Note 4 to Category 5 Part 2, which gives us that primary function test.

The 992, so if your item is not out of Category 5 Part 2, you can maybe get out of going to the 002 party by being a 992 item. So some decontrols or exit strategies to be considered in the 992 bucket would be if your key length is less than 56 bits for symmetric encryption, less than 512 for asymmetric or 112 elliptic. Also, if your item is using encryption for authentication only, then your product could be under 992.

I will also go through several decontrols that we have listed in our regulations under Category 5 Part 2, which essentially say if you're using encryption for the following functions that are listed in the decontrol, they will not be controlled at the 002 level, they'll be controlled at the 992 level. And then mass market, Aaron will talk a little bit further about mass market.

So the last thing I'd like to talk about in this slide is that the 002 controls go hand in hand, for the most part, with license exception ENC. So I will address most -- the chunk of the presentation, my part of the presentation, will be talking about the 992 controls and how you can get there before getting to a 002 control.

So up front we discussed Note 4, the primary function test. So if your item qualifies for Note 4, it's described under Note 4, then is it not in Category 5 Part 2. They wouldn't even get a 992 control under Cat 5 Part 2. It would be out of Category 5 Part 2 in another category if it falls there, or EAR99.

So this slide summarizes Note 4. It says Note 4 excludes from encryption controls items whose primary function is not computing. So it's not a general purpose computer, not a laptop, not a processor, not a single-board computer, primary function is not computing. Also, it's not -- or it's not communication. Communications, like it's not a phone, it's not a fax machine, it's not a transmitter or receiver, not a modem, not an e-mail application, not a general purpose SMS messaging application. Those are all primarily used for communication.

Or it's for networking. Networking items are like routers. It's not a router, it's not gateway, firewall or software that runs on these items. It's not network management software. Those products are primarily used for networking. And not for information security. So it's not a secure storage device or drive, and the software that's used to encrypt information, or network analytic tools.

So those are some examples that I've listed through whose primary function are for computing, communications, networking, or information security. The decontrol note applies to when the primary function is not one of those. So it's written in a negative, so that's how we should apply it.

So the best thing, actually, to talk about Note 4 is to dive into some examples. So here we've got some examples of what we do consider Note 4 items. So when the primary function is for copyright protection or software licensing, then it can be considered Note 4. Games or gaming also note 4 items. Household utility and appliances like connected home, smart home, software and hardware associated with that, where the primary function is for household utilities and appliances can be considered under Note 4, and decontrolled by note 4 and out of Category 5 Part 2; printer, copiers, not fax machines, because a fax machine's, primary function is communications there. Imaging and video recording equipment, so this can include surveillance cameras. But this does not extend to video conferencing because video conferencing's primary function is communication. So that would not -- video conferencing software, for example, may not be decontrolled by Note 4.

We also cover, under Note 4 -- things that would be decontrolled by Note 4 would be business process modeling and automation. So supply chain management software, inventory software, scheduling and delivery software. Note 4 can also apply to industrial controls, things that are used on the manufacturing floor or used to control mechanical systems, robotics, or things that are used to automate a factory and secure communications within a facility, such as for fire alarms or HVAC. Encryption used for those functionalities and those products can also be considered Note 4. We also see a move towards smarter cars, so those types of software and hardware can also be decontrolled by Note 4, aviation software or transportation systems.

Before I leave this slide, I'd like to just go through maybe a little example. So let's say we have a connected home with lighting controls that you can manage from your phone and you have an app on your phone that is used to control the lights in your home, and the data going from your phone to the lights are encrypted. You're using secure communications. So the question is whether the app on your phone that's used to control the lighting in your home would be Note 4. Well there is some underlying communication there to communicate with the light bulbs or the smart devices in your home, but the primary function is for, like we said, it's for controlling, it's for home automation. So if the primary function is home automation, the communication is there to support the primary function of home automation, so using the primary function test, we see that it is not for computing. The primary function is not for communication. The communication is more of a secondary or in support of function, not for networking, and not for information security.

So with the primary function being home automation, we could consider the app on your phone under Note 4, and it would not be controlled under Category 5 Part 2. What about the phone itself? The phone itself is primarily used for communication, not an item that would be subject to the Note 4 decontrol, or even the wireless router you may be getting internet access from to your phone would not be considered under the decontrol, of the Note 4 decontrol because it's primary function is for networking and/or communication.

So like I talked about, the 002, I've got a little man running for an exit door here on this slide. This slide talks about authentication only. So if your item is using authentication only, you would not be -- if it's using encryption for authentication only, you would not be controlled under 002; rather, use that exit door and go to the 992. So when we talk about authentication, if your product is using encryption for authentication only, we're talking about encryption that's used for things like passwords or PIN numbers or things are used -- data that would be limited to -- that is used for access to a system would be considered under this note. So, again, those passwords and PIN numbers and similar data that would prevent unauthorized access to a system is what we consider authentication. So if your product is using encryption for authentication only, then use that exit door to the 992.

Now I'm going to talk about several decontrols that we have in our regulations, and these decontrols are found under 5A002. We have about eight or nine here that I'm going to talk about. The decontrols, again, allow you to go from a 002, or, rather, never get to a 002 control. You'll have that low-level 5A or 5D992 classification. So the first one under the decontrol notes -- and these decontrol notes can be found in Category 5 Part 2, actually under the entry of 5A002, and it will say -- it says these items are not controlled under 5A002, so they will be controlled -- they are controlled under 992.

And it starts off with the personalized smart cards and smart cards readers. So this could include the smart card itself, the readers, the writers, and these are cards that are specially designed and limited to allow protection of personal data. So that includes any data that is specific to a particular person; for example, the money that's being held within the account that the smart card is being used for.

Decontrols b through c are reserved, so going down to decontrol Note d is designed for money transactions and banking use. So this is limited to when the encryption is limited in your product to encrypting, for example, credit card transactions, encryption that's associated to the settlement of fairs or other credit functions.

The next note refers to mostly cordless telephones. Note g refers to customized client wireless devices that are customized for civil use, so an example here, smart phones. A smart phone that is used by your utility meter reader who comes by and scans your meter every month. That device may also have Internet connectivity. It may also be able to place phone calls, because it is a smart phone. But it's been customized for this civil end-use for all the utility meter readers in the city to carry when they are doing their work out in the field. So that's an example of something that could be decontrolled when it's customized for a specific civil use, and the item does not fit under the decontrolled for Note 4 example, because it's still a phone, it still can place call, it can still have internet action. So this Note g allows us to decontrol those sorts of items that are customized for civil use.

Moving on, the next note is the wireless PAN note. So the wireless personal area note is limited to items that have a range of 30 meters, according to the manufacturer's specification, or if it's limited to a hundred meters for equipment that cannot interconnect with more than seven devices.

Note j talks about encryption that is not used, that cannot be used in the product. So as long as the encryption in your product cannot be written to, cannot in the future be written to or enabled, it is the equivalent of blowing a fuse to the encryption functionality in the product. It is there but it is not going to be used, and it will never be used. It can go under Note j.

Now there's a second part to Note j that talks about dormant encryption. This is encryption that is in the product but it's not activated. But it can be later activated; for example, if someone pays a license fee, an additional license fee to enable the encryption functionality that's in the product. So this allows for a mechanism to decontrol down to the 992 level of products that have encryption but is not being used or is not activated.

Note k talks about small-cell equipment. So this is mobile radio access networking equipment that's designed for civil use. Note l and m were more recently added, and I'm going to take the next couple slides to talk a little bit more about them since they were recently added, and they do encompass a new terminology, a terminology that was added for the operation, administration, and maintenance, which has a definition in Section 772. So that decontrol Note l, was added in May of 2015, and it's for routers, switches, and relays that use encryption only for operations, administration, and maintenance.

There's a definition, again, in 772 of the EAR that specifies what we mean by OAM. The gist of it is that if the encryption is used to set up and start an appliance; for example, managing account privileges of the user or administrator, or the settings of the item, or Part B discusses keeping the appliance running, so monitoring or managing the operating conditions or performance of the item. Part C discusses the logs, the data logs, audit data that could be used for Part A and B.

Currently this decontrol does not extend to storage appliances or firewalls. So if you think this decontrol applies, I encourage you to look at the definition of OAM in the regulations. And also keep in mind that OAM is not for items that encrypt data. We're talking about encryption that is limited to what we call the control plane for management data only. Also note that while this decontrol refers to routers, switches, relays, mostly hardware items, there is also a corresponding software decontrol, which can be found under a note to the entry of 5A002.c.

And lastly Note m, decontrol note M, which was also added at the same time, in May of 2015, it refers -- it's a slightly broader note, but it also encompasses the OAM definition. It extends to computers and servers where the encryption is integral to a mass market processor or an operating system. I like to replace the word "it's inside of" in place of "integral to" when I read the regulations, because it makes more sense to me.

So essentially you have a general purpose computer or server where the encryption functionality is inside of a mass market processor, then this decontrol note could apply. Or if the encryption functionality is inside of just the operating system, that is a mass market operating system, then the decontrol could apply. And then lastly, if you have a general purpose computer or server that is limited to operations, administration, and maintenance, as we discussed, and as is defined in Section 772, it can also be decontrolled from this, using this note.

So with that, I've discussed several off ramps to before getting to the 002 control. The decontrol notes, if you're using authentication only, if you're less than the key length specified, then you can end up in a 992 classification. And then we also covered items that are not subject to Category 5 Part 2, mostly Note 4 items.

And then so now I'm going to pass it over to Aaron who is going to discuss 002 controls. And as I mentioned, the 002 controls go hand in hand with license exception ENC, which Aaron is going to discuss in greater detail next.

Thank you, Anita. I'm going to talk now about license exception ENC. So if you've gotten this far in the analysis, you've gone through all of the references which Anita just talked about, the decontrol notes and the Note 4, and the product doesn't fall under any of those, then you know that you're in license exception ENC and mass market.

So the table that you have in front of you summarizes all the provisions of license exception ENC. This chart is available as a handout on your screen, and there's also a similar one for mass market products -- for the mass market authorization that's available to you.

As you can see from the chart, there's a lot of different authorizations and provisions in license exception ENC. But in the end you can export almost all encryption products almost anywhere in the world under license exception ENC. The difficult part of ENC is determining which of these paragraphs the product or the transaction falls under and then what the corresponding regulatory requirements are for that provision.

So the chart has six different types of authorizations in the six rows. The rows that are in blue on the chart are the instances in which you can export under ENC without any prior authorization. No registration, no classification is required. If the product doesn't fall or the transaction doesn't fall under one of those, then the next place that you look is in Paragraph (b)(2), and (b)(2) is the most restrictive paragraph in ENC. (B)(2) items require the encryption registration, the classification request, and they also have a semiannual sales reporting requirement. Then even after all of that, there are some instances in which you may need a license for (b)(2) products.

If the product doesn't fall under (b)(2), then the next place that you look is Paragraph (b)(3). (b)(3) is the next most restrictive paragraph, and the (b)(3) items also require an encryption registration, and they require a classification request, and a few of the items in (b)(3) also require semiannual sales reporting, but not all of them, only a few.

Then once you do that, the authorization under (b)(3) is much broader than under (b)(2). And then finally, if the product doesn't fall under Paragraph (b)(3), then the default is (b)(1), and (b)(1) only requires the encryption registration, and it also has a very broad authorization that's available for it.

First we'll go over the instances in which you can export without any encryption registration or classification under license exception ENC. The first provision is 740.17(a)(1). And (a)(1) allows you to export to private sector end users that are headquartered in a Supplement 3 country, but for a very narrow end use. It has to be for the development or production of new products, only for that end use.

"Private sector end user" is defined in the EAR. Basically a private sector end user is a private company that is not owned or controlled or acting on behalf of the government, so basically a private company. And then Supplement 3 is also a term that we'll see in the next slide. Supplement 3 countries are basically the EU, plus a few other friendly countries. So basically the EU plus a few countries. So (a)(1) allows you to export to basically private companies that are headquartered in the EU, plus a few other countries, as long as it's for the limited end use of development or production of new products. So that's (a)(1).

(A)(2) is, in some ways, a little bit broader than (a)(1). (A)(2) authorizes exports to U.S. subsidiaries as long as its for their internal use. And "U.S. Subsidiaries" is also a defined term in the EAR. Basically a U.S. subsidiary is the overseas office or subsidiary of a company that is headquartered in the U.S.. And it doesn't have to be the exporter's subsidiary, it just has to be the subsidiary of a company that is headquartered in the U.S. to take advantage of that provision. This provision also authorizes exports to employees, consultants, and interns of U. S. companies. So the provision is available for exports to overseas employees, overseas consultants, and interns of companies that are headquartered in the U.S.

And then the last provision under ENC which you can export without prior authorization, no registration or classification, is Paragraph (b)(4), and (b)(4) applies to certain short range wireless products. And (b)(4) has become somewhat redundant in the regulations these days, because there's the decontrol notes that Anita talked about earlier and Note 4 that already decontrol the products that are described in (b)(4). So (b)(4) is still there in the regulations, but it's a little bit redundant now.

I mentioned the Supplement 3 countries in the previous slide, and this slide explains what the Supplement 3 countries are. It's basically the EU, plus eight other countries, like Australia, Canada and Japan, Norway, New Zealand, Turkey. There's 33 countries total in the Supplement 3 countries. And Supplement 3 is a term you'll here a lot in license exception ENC, because the requirements for license exception ENC often vary depending on whether you're exporting to a Supplement 3 country versus outside the Supplement 3 countries. Basically there are fewer restrictions on products that are going to the Supplement 3 countries. So you can think of the Supplement 3 countries as basically the EU, plus a few other countries.

Now if you've gotten that far and the product doesn't fall under any of the provisions that don't require any registration or classification, then the next place you have to look is the in Paragraph (b)(2). Paragraph (b)(2) is the most restrictive provision in licensing exception ENC. These are mainly network infrastructure items, along with certain other specialized commodities and software. It also includes source code, encryption source code and encryption technology. (B)(2) items have more restrictions on them, so if you have a (b)(2) item, there may be some cases in which you'll need to come in and get a license. But the requirements for when a license is required for (b)(2) items are different, depending on the product that it is, who you're sending to, and what country it's going to. So the license requirements vary depending on those factors. The (b)(2) items require a registration and a classification to be eligible license exception ENC, and there's also semiannual sales reporting that's required for (b)(2) items.

The first part of the (b)(2) items is the network infrastructure criteria. This provision covers certain network infrastructure products that exceed the criteria that you can see on the slide here. Mainly this would apply to enterprise and carrier class, routers, switches, base stations, VPN and network gateways, security products, those types of things. It generally won't apply to client devices, and it won't apply, generally, to local area network equipment. It is mainly for enterprise and carrier class network infrastructure equipment. The criteria also don't apply to products that only use encryption for management function, either network management or device management functions. If the only thing encryption is used for is management functions, it won't fall under this (b)(2) criteria.

All of the items that are described on this slide under ENC require licenses if they're going to government end users outside the Supplement 3 countries. So once you do the encryption registration and the classification that's required, you can export under license exception ENC everywhere except government end users outside the Supplement 3 countries.

Now (b)(2) also has a few other things in it that are not network infrastructure items. They get caught by the (b)(2) criteria, as you can see in the list on the slide in front of you. Encryption source code falls under (b)(2). This is proprietary encryption source code. If it's open source publicly available, it doesn't fall under (b)(2). But if it's proprietary encryption source code, then it falls under (b)(2).

The next one is products that are designed or customized for government end users. This is for products that are designed to be useful, primarily useful for government customers. The main thing that we see under this provision is products that people design for police or first-responder use.

Next one is if you're customizing the cryptography for a particular customer, that puts it under (b)(2). The next two. products that perform quantum cryptography and products that are customized for supercomputers, those fall under (b)(2). Those are very uncommon. We don't see things under those two provisions very often. Now, also penetration testing products, if you have a penetration testing product that has encryption, that falls under (b)(2). And then first responder, public safety radio, which is primarily TETRA and P25 radios.

So all of the items that we just talked about, from the encryption source code through the first responder, public safety radios, the authorization for those items is the same as the network infrastructure items. So those require licenses if they're going to government end users outside of the Supplement 3 countries. But once you've done the encryption registration and classification, it can go under ENC to other types of end users.

The last two items on the slide have slightly different authorizations than the rest. First, cryptanalytic items require licenses to all government end users, except Canada. Even the Supplement 3 government end users would require licenses for cryptanalytic items. And cryptanalytic items, the main thing we see there is password guessing products. So cryptanalytic items require licenses to all government end users.

And then the last one on the slide is open cryptographic interface or OCI. OCI items require licenses to any end user outside the Supplement 3 countries. So it's pretty restricted under license exception ENC. An OCI is basically where the developer leaves the programming interface open for the encryption that would allow somebody to basically reprogram the encryption and insert whatever encryption they want without the manufacturer's assistance. Those are also pretty uncommon in our experience, but we do see them occasionally.

The last thing that is in (b)(2) is technology. And as many of you probably know, when we're talking about technology we really mean development and production technology for the encryption functionality. And license exception ENC breaks technology down into basically two categories. The first is technology for non-standard cryptography. And technology for non-standard cryptography requires a license to any end user outside the Supplement 3 countries. So, again it's pretty heavily restricted under license exception ENC.

The definition -- there is a definition for "non-standard cryptography" in the EAR. Non-standard cryptography basically means any cryptography that's not part of a standard -- a published standard or that's not otherwise published, information on the algorithm is not otherwise published. The things that we typically see as non-standard cryptography are somebody developing their own encryption algorithm that's not published anywhere. They develop their own algorithm and want to use that. And the other thing is WAPI, which is a Chinese wireless encryption protocol. Those are the two main things that we see as non-standard.

If you're using common standard algorithms like AES, DES, 3DES, those are all standard cryptography, and that wouldn't get caught as non-standard. But the technology for developing non-standard and producing non-standard cryptography under ENC would require licenses to any end user outside the Supplement 3 countries.

The second type of technology under ENC is what the regulations call "Other technology," and other technology means technology that's not for cryptanalytic items, not for non-standard cryptography, and not for open cryptographic interface. So it's kind of the default technology, for encryption technology that is none of the above. And that technology has a much broader authorization. That technology, other technology, requires licenses to country group D:1, any end user in country with D:1, and to government end users outside the Supplement 3 countries. Otherwise, again, once you do the encryption registration and classification it can go to other type of end users under license exception ENC.

That's it for the (b)(2) criteria. If your product doesn't fall under any of those (b)(2) criteria, the next place you want to look is (b)(3) - 740.17(b)(3), and (b)(3) is called -- you'll see this called ENC unrestricted. Sometimes you'll hear people refer to the (b)(2) items as restricted items, ENC restricted items. Companies will say, "I have an ENC restricted item." They mean 740.17(b)(2). And then if they say, "We have a ENC unrestricted item," that's usually referring to Paragraph (b)(3). So that's a slightly different terminology that's used sometimes.

And the (b)(3) products include the list that you see, products that you see in front of you. If the product meets the (b)(2) criteria, it falls under (b)(2). But assuming it doesn't meet the (b)(2) criteria, these products would then fall under (b)(3). The first one is a components. Components with encryption functionality will fall under (b)(3). Development kits and toolkit with encryption, fall under (b)(3). Cryptographic enabling items, these are items where you have a product that has encryption that is dormant or inactive and you have a license that enables -- activates that dormant encryption functionality. That licensing mechanism is a cryptographic enabling item. And if it doesn't fall under (b)(2) then it falls under (b)(3).

Next is commodities with non-standard cryptography. Again, if you have a product with non-standard cryptography that meets the (b)(2) criteria, it falls under (b)(2). But if it doesn't meet the (b)(2) criteria, then it falls under (b)(3).

And then the last two items, certain types of forensic, computer network, forensic products, and network analysis and packet inspection equipment that is adapting the real time to the operating environment, and those two item haves particular requirements. They're in Section 740.17(b)(3)(iii). So you'll hear me call those products the (b)(3)(iii) items. It's not all forensics products or packet inspections product, only certain ones that are described in those paragraphs, and those items have slightly different authorization requirements than the other (b)(3) products.

The (b)(3) items require a registration and a classification to be eligible for ENC. But once those are done, they are authorized. The authorization is much broader. It can go to any destination except the five embargoed countries. So it's a fairly broad authorization. And then in addition, the (b)(3)(iii) items have a semiannual sales reporting requirement, but the other (b)(3) items don't have any reporting requirements associated with them, just those (b)(3)(iii) items.

If the product doesn't fall under (b)(3), then the default, as I said earlier, is (b)(1). And (b)(1) is anything that doesn't fall under the (b)(2) or the (b)(3) paragraphs. And (b)(1) items only require the registration to be eligible for ENC. A classification is not required for those items, only the registration. And once you have the registration, they can go under license exception ENC, again, anywhere except the embargoed countries. So it provides a pretty broad authorization with just the encryption registration.

And that's it for license exception ENC. Now I'll talk about the mass market requirements. Mass market is -- the authorizations for mass market are very similar to the ones for ENC. It's almost the same authorization. The main difference is that the products that fall under mass market have to meet the mass market note. The mass market note, you'll see on the slide, it says cryptography note. We use the two terms sort of interchangeably, mass market note and cryptography note are the same thing. I think even in the slides you may see them stated both ways, mass market, cryptography notes, the same thing.

There's two parts to the cryptography note. Part A is mainly for finished products, and sometimes it can be for components, but it's mainly for finished products; and then Paragraph (b), which is for components, encryption components. And Part A, under Part A it says the product has to be generally available to the public, being sold without restriction from stock at retail selling points. The cryptographic functionality cannot be easily changed by the users, and it has to be designed to be installed without substantial support from the supplier.

Those provisions are somewhat broad and open to a lot of interpretation, so in addition to that, we have a note to the cryptography note that explains some of the things that we look for in deciding whether something meets that cryptography/mass market note. The first one is that the item has to be of at least potential interest to a wide range of individuals and businesses. If it's something that would only be of interest to a very small group of people, it probably won't qualify for mass market.

The next one in (1)(b) basically says that you have to be able to find out basic information about a product without the need to contact the manufacturer. If the manufacturer doesn't provide even basic information to the public about their product, you have to call them up and talk to them, and then they can tell you that they have this product. That's not really something that is mass marketed. So you have to be able to find out basic information about the product without needing to consult the vendor or supplier.

And then the last paragraph provides some of the factors that we take into account when determining whether something qualities for mass market. And there's no black-and-white lines that we draw with these. We just kind of weigh these factors together in determining whether something qualifies for mass market. So we look at quantity, the amount that's been sold, that you sold, you know, in the U.S.; the price, if it's really high or really low; the required technical skills; if you have existing sales channels, the products that you've already been selling in the mass market, who typical customer is, if it's a general consumer or somebody that's very specialized, and typical use, and any exclusionary practice of the supplier, if the supplier will only sell to certain segments of customer, things like that.

And so the basic idea is if you've already sold a lot of a product in the U.S., the price is very low and it's something that, you know, everybody can use, you don't need very much skill to be able to use it, that's something that's more likely to be mass marketed than something that you haven't sold any of,it's really, really expensive and it requires a high amount of technical skill to be able to operate it. That's the basic idea with those criteria.

Paragraph (b) of the Cryptography Note is for components. And Paragraph (b) says even if the component doesn't meet Paragraph A, which most components don't, it can still qualify for mass market, as long as it is a component of a mass market product. And under Paragraph (b) we mainly put two types of products. First is, if it's a component of an existing mass market item, that's the factory installed component of a mass market item. So if you have a cell phone, a Smartphone and it's using chip A and you want to export chip A, that's the factory installed mass market component of a mass market item, so that should qualify for Paragraph (b).

The second type of component that we put under Paragraph (b) is a product that is a functionally equivalent aftermarket replacement for the OEM component. It's not the exact chip A that's in the mass market mobile device but it's functionally equivalent. It does basically the same thing as that chip. So those are the two main things that we put under Paragraph (b).

Paragraph (b) also applies to software components. So modules, libraries, firmware that runs on components. Those are all eligible under Paragraph (b). One major limitation to Paragraph (b) is that, if the primary function of the component is information security, then it doesn't qualify for Paragraph (b). So on the hardware side this means that things like cryptographic accelerators wouldn't be eligible for Paragraph (b), and on the software side, encryption libraries would be an example of something that wouldn't qualify for Paragraph (b), even though it's a component. So that's one big limitation of Paragraph (b).

The next thing I'll talk about is mass market authorizations. The mass market authorizations are very similar to the ENC authorizations, as I said. The main limitation is that it -- the main difference is that it becomes a 992 item if it meets mass market criteria instead of an 002 item. So if it starts out as 5A002, it meets the mass market criteria, it becomes a 992 item.

One other major difference with ENC is that the items that are described in 740.17(b)(2) and in (b)(3)(iii), the forensic and network packet inspection products, don't qualify for mass market. So if you have one of those products that fit under those provisions, then those won't qualify for mass market. But otherwise, other than that, the authorization under mass market and ENC are pretty much the same. You have a (b)(3) mass market provision, just like you have an ENC (b)(3) provision, and it applies to the same products; components, non-standard cryptography, development kits, et cetera.

And just like with ENC, those items require an encryption registration and a classification, and once those are done, they can be exported anywhere except the embargoed countries. And, again, just like with ENC,if it doesn't fall under (b)(3), then it defaults to Paragraph (b)(1), and (b)(1) only requires the encryption registration, and once the registration is in place, it can be exported to any destination except the embargoed countries. And as I said at the beginning, there is a chart in the handout that provides another table with the different types of mass market authorization.

Now we've gone through all of the different authorizations that are available for -- under license exception ENC and mass market. So that's all of the different authorizations that are available. And now I'm going to talk about once you figure out whether you need the registration, the classification, or the reporting, the mechanics of how you do that, how you submit the different forms that are required.

First is the encryption registration. And as a reminder, the encryption registration is required for all of the (b)(1), (b)(2), and (b)(3) items under both ENC and mass market. The encryption registration is a separate module in SNAPR called the "encryption registration." You fill out the encryption registration form in SNAPR and you attach the Supplement 5, the answers to the questions that are in Supplement 5 to Part 742. You attach that in SNAPR and then you submit it. And then the system will basically automatically send you back the encryption registration number, and that's it. That's the entire process for getting the encryption registration.

The encryption registration is really a company registration. It's not a product registration. So the regulations only require you to submit one registration per company. And the registration only needs to be updated once a year. That's a calendar year. Once per calendar year, and only if something changes in the registration. So the most you should ever have to submit an encryption registration is once a year, and then only if something changed in your registration from the previous year.

If you are not the manufacturer of an item you can rely on the manufacturer's encryption registration, if they have one. If you want to export a (b)(1) product and you don't have an encryption registration but the manufacturer had told you they have an encryption registration, then you can rely on the manufacturer's encryption registration. You wouldn't need to submit one of your own. That's the registration requirement.

The classification requirement, again, the classification is required for items in (b)(2) and (b)(3) of ENC, and mass market (b)(3). For the classification request, you fill out the same commodity classification request form in SNAPR and then you attach a data sheet or equivalent, something equivalent to the data sheet. And you provide the answers to the questions that are in Supplement 6, to part 742. Those are all the questions on the encryption functionality. And then you submit that.

And once you submit the complete review request, so the review request with the data sheet and the Supplement 6 information, once you submit the review request, you can start exporting immediately to the Supplement 3 countries. You don't have to wait to hear anything from us. You can export immediately to the Supplement 3 countries. Then, 30 days later, you can start exporting under the full authorization of license exception ENC, even if we haven't issued the classification yet. And the 30 days doesn't include days that we've put the application on hold, but if you submit a classification request and 30 days go by and you haven't heard anything from us on the classification, then you can start using license exception ENC under the authorization that you requested.

Once you have a completed classification request, and we've issued the classification request, a new classification is only required if you make changes to the encryption functionality of the product. So you can make other changes to the product. You can change the name of the product. You can make other changes that don't affect the encryption, and you don't need to come in for a new classification request for that. You only need to come in for a new classification request as soon as you start making changes to the encryption functionality of the product.

And the last thing that I'll talk about, then, is the reporting requirements. Now under the license exception ENC in mass market there's two types of reporting requirements. The first is the semiannual sales report, and that's required for the (b)(2) items and the (b)(3)(iii) items, the forensic and packet inspection network analysis products. Those require a semiannual sales report. You have to basically report each transaction that you made under those provisions. The reporting for the semiannual sales report is only required for exports from the U.S. and for re-exports from Canada. So re-exports from other countries don't require any reporting, only exports from the U.S. and from Canada.

There's a few exceptions to the reporting requirements also, which you can see in 740.17(e). And for this report, the semiannual sales report, there's no specific formatting requirements that are required by the regulations. As long as you provide the information that it asks for you can put it in whatever format works for you.

The other type of reporting is the annual self-classification report. And self-classification is a little bit of a misnomer. It's not really just for products that you self-classified, it's required for all (b)(1) items that you exported under your own encryption registration number. And it's not a transaction report, it's just a report that lists the products that you have been exporting under Paragraph (b)(1). And that report has specific format requirements. It has to be in a CSV format with six specific data fields. And all the details for that are in Supplement 8 to Part 742 of the EAR.

And then the last thing I'll note is that, as you can see, there's no reporting required for any of the (b)(3) items except for the (b)(3)(iii) items. But the other (b)(3) items don't have any reporting requirements that are associated with them. And with that, I'll turn it over to Randy.

Thank you. We have two quick topics to cover before we start taking questions and answers. The first topic is encryption licenses and encryption licensing arrangements. Now as we've heard from Anita and Aaron, a lot of products, a lot of transactions are eligible for either decontrol under mass market or for license exception ENC. So what we're left with, for licensing purposes, are those restricted (b)(2) products that are being exported to government end users, for the most part in non-Supplement 3 countries.

We also have encryption licensing for encryption technology for the development and manufacture of encryption products abroad and, of course, there would be licensing required for exports to the embargoed countries. Those licenses, our division doesn't handle. They are handled by the foreign policy division.

As a general matter, our approval rate for export licensing is very high. There are very few end users or destinations that are problematic. In fact, the licensing is more for making sure we know what is going where, as opposed to trying to control it from going there. So, generally, we have a very high approval rate for our export licensing.

Now, as we heard from Aaron, the license exception ENC authorization is generally to non-government end users, so the licenses are required for government end users. And we do have a definition of government end user in the regulations in Section 772.1. As a general chapeau, the definition would encompass any foreign central, regional, or local government departmental agency or other entity performing governmental functions, including research institutes, and also companies that are owned by the government that manufacture products on the Wassenaar Munitions List.

Our definition of government end user does have a number of exclusions. It wouldn't be an encryption provision if it didn't have several layers. And the exclusions include utilities, including telecommunications and internet service providers; banks, financial institution; transportation entities such as government-owned airlines, or government-owned railroads, government-owned entertainment organizations; educational organizations. But this exclusion does not include research institutions or public schools and universities. And finally, the last exclusion is for civil health and medical organizations.

So none of those are considered to be government end users, and people, exporters do have problems often, with trying to determine under this definition whether a particular foreign entity would or would not be considered a government end user under the definition. We do consider it our responsibility to make that determination, so if there's a question about an entity, please feel free to e-mail us with whatever information you have, or a website, and we'll look at it and try to decide whether we would consider it a government end user or not.

If there simply isn't enough information to make the determination, we would default to determining that it is a government end user. But in many situations we can provide our written determination that an entity is not considered a government end user under this definition; therefore the transaction would be eligible for license exception ENC.

Now because we have a large quantity of export licensing for encryption products, although we do offer the normal individual validated license, which is for a specified quantity of products to a specific end user, we also have a vehicle called an "Encryption Licensing Arrangement," which is mentioned in the regulations but isn't really discussed very thoroughly, and has sort of grown up on its own as a practical matter as opposed to a regulatory vehicle. An Encryption Licensing Arrangement is available for unlimited quantities of products, may include a long list of products, and may be for a range of end users as well.

Generally speaking, the Encryption Licensing Arrangements are for a four-year validity period, and over time we have developed two different kinds of encryption licensing arrangements. We've divided government end users into two different lists, less sensitive and more sensitive. For the less sensitive government end users we offer what we refer to as "Worldwide ELAs." They do not include authorization to the embargoed countries but to all other destinations. And this is one license that we issue for all of these destinations. The licenses, as issued, have various end users and in various countries. That's how the license reads.

And for those Encryption Licensing Arrangements, the condition is usually a semiannual sales report, which is, as we know, very similar to what is available for non-government end users for (b)(2) products under license exception ENC. So the difference between a worldwide Encryption Licensing Arrangement and licensing exception ENC authorization is very small.

We also have a list of more sensitive government end users. And to date, we've only been able to issue these for one country at a time. So we also refer to these as "Single-country ELAs." The condition on these authorizations is generally a 15-day pre-shipment notification. The notification is submitted by e-mail to both BIS and to NSA, and it doesn't mean that we all come back and say, "No, you can't ship the product." The notification is also there. It's simply a notification to say we're sending this product to this end user in this country.

So the two handouts that -- two of the handouts that were included with the materials include these lists of less sensitive and more sensitive government end users. And, to date, we have been able to place any government end user that we have run across in one of these lists. There may be a time when I can't say that, but, to date, we've been able to find a paragraph to put every government end user that we have identified. And we encourage the use of the ELAs, both to save time for exporters and to save time for us with processing license applications.

The last topic that I'll touch on for purposes of this webinar is publicly available encryption software. Anita mentioned publicly available encryption items as not being subject to the Category 5 Part 2 controls. In fact, we do retain jurisdiction for encryption source code. It does remain classified under ECCN 5D002, even if it is publicly available. And the statement of this retention of jurisdiction is set forth in Section 734.3 of the regulations.

This does not apply to publicly available encryption technology. Technology can be made available and published, and it is not subject to the EAR. But source code is, to date, still subject. However, it is not restricted and can be exported under licensing exception TSU, or Technology and Software Unrestricted, after a notification is submitted by e-mail to BIS and to the National Security Agency. That notification states where the source code is posted on the Internet, or the notification can be a copy of the source code that's posted.

Object code that's compiled from source code and made eligible for license exception TSU, and that also meets the publicly available criteria set forth in Section 734 becomes not subject to the regulations. And publicly available mass market encryption software is no longer subject to the EAR. But I included this slide because in order for a mass market encryption software to be publicly available and not subject to the EAR, the process for making it mass market to begin with has to be followed. So the process is to submit an encryption registration and to self classify the mass market software, and then to make it publicly available so it is no longer subject to the regulation.

I've included one more slide just sort of bringing us back to the beginning here, Anita's discussion of the Category 5 Part 2 controls. We often run into situations where exporters don't believe that their product is subject the regulations because it's only using open-source software. Now back to Anita's discussion, what we control under Category 5 Part 2 are items that are designed or modified to use encryption. So it doesn't matter that the software that's being used is open source, it matters what the product is and how it uses encryption. So based on that, the use of open source software doesn't itself affect whether or not the product is itself subject to the regulations and subject to Category 5 Part 2.

So that completes our topics for today. We have an encryption page on the BIS webpage. Unfortunately, I've learned, since we created these slides, that this link is not correct, so please don't try to use it. If you go to bis.doc.gov and look under policy guidance, one of the choices for policy guidance is encryption. So that will take you to the list of guidance charts, forms, and FAQs that we have listed there, and probably as of tomorrow, this webinar as well will be posted.

We also have a helpline for the division that you're welcome to call at any time; that's here on the page. And finally, this is the contact information of all of the licensing officers in the division and their e-mail addresses and direct phone numbers. So please feel free to call us with questions that you may have as a result of this webinar or in the future. Thank you very much.

We'll go to questions and answers for the next ten minutes. We have some questions that have been posted here, and one of the questions that was asked most frequently was, "Will the slides be posted for the attendees to print?" And the answer I received is that they already are included in the materials, along with the handouts that were provided. So if you have any problem finding those, please let us know, and we'll be sure that you receive them.

So the first question that we received asks about the software that is specifically designed or modified for a government end user. And the question is, "Is it just the encryption or it is the software application that would be subject to the (b)(2) paragraph of license exception ENC?"

And the answer to that is it's really both. If you're customizing encryption functionality for any particular customer, an individual customer, government or non-government customer, it would fall under (b)(2). But, of course, if you're customizing it for a government customer, then under (b)(2) that means it would require a license to government end users outside the Supplement 3 countries.

But apart from that, if you were customizing the rest of the product for a government customer, then that would also put it under (b)(2). If you're customizing it for non-government customers, if you're customizing things other than the encryption for non-government customers, that wouldn't necessarily put it under (b)(2). But if you are customizing some kind of product for a government customer, even if it's not related to the encryption, then that would put it under (b)(2).

Another question that I think you would best answer, Aaron, "Would software code that decrypts encrypted data be covered; for an example, software that opens encrypted PDF files?"

Yeah, so that's a good question. Decryption under the regulations is really treated exactly the same as encryption. The regulations don't really make any distinction between encrypting and decrypting. So assuming that a product wouldn't meet -- doesn't meet one of the decontrol notes or meet Note 4, or one of the other releases, then that would be controlled, just based on the fact that it's using decryption. Because decryption and encryption are treated pretty much exactly the same under the EAR.

Here's a question related to Paragraph (a) of license exception ENC. "How do you determine where the headquarters of a company is if the subsidiary is in China but the parent is in Germany? Where do you determine to be the headquarters, or are headquarters and parent company locations to be used interchangeably?"

Yeah, that's a good question that we get a lot. There's no definition of what "headquarters" means for purposes of Paragraph (a). And what we really look at is where the company says their headquarters is. We look on the company's website and we look at where they say they're headquartered. So that's basically what we use. So if they're advertising themselves to the public as a company that is headquartered in a Supplement 3 country, then that's probably how -- that's how we would treat them.

And here is a Note j issue. This is decontrol Note j to 5A002 that provides -- that equipment with encryption functionality that cannot be used is decontrolled from 5A002. And the question is, "What is meant by 'cannot in the future be used' in the decontrol note?"

Yeah, for decontrol Note j, the analysis can be a little bit complicated. The note says that it decontrols products where the encryption either cannot be used or can only be made usable by cryptographic activation. And the cryptographic activation part, I think, is a little bit clearer. There's a definition of cryptographic activation. So if you've made the encryption dormant or inactive and you have a license key that you provide that's linked to the individual product or the customer so that the person that gets the license can only activate it on that specific product, they can't share it with other people to activate encryption, it's only useful on that product or that customer's product, then that would qualify under the decontrol Note j. The encryption is dormant and can only be made usable by means of cryptographic activation.

Then you have -- the other part is for encryption that cannot be used, and there's really, I think, two distinctions there. One is if the encryption is there, but it's made completely unusable so that nobody can use it, even if they wanted to. It's physically impossible for somebody to use it. The example we always use is, you have a chip within encryption block and somebody cuts the line into the encryption block so that you could never use the encryption again. In that case we would treat it as not having encryption functionality at all. We would treat it as not an encryption product.

But if the encryption is there, and it can be used, it's possible, it's physically possible to use it, there has to be some mechanism in place that you put that's not quite an encryption license, a license for activating the encryption, but some mechanism in place to make that encryption not usable, even if somebody wanted to use it. So that's kind of where we would draw the line with encryption that cannot be used.

Thank you. I'm getting signals that our time is up. We haven't answered all of the questions, but please feel free to provide them, and we will have a record of these questions that were asked and try to post frequently asked question on our website shortly. Thank you very much for attending this webinar, and we look forward to talking with you.