

Encryption Workshop Update 2011 (Part 2)

July 21, 2011

>> Randy Pratt: If you could take your seats, please, so that we could resume... Thank you very much. We received a number of questions about the material that Anita covered in Note 4, so we'll start with her response to a number of those questions, and Judy will also take a few of them. If we -- At some point, we'll save the rest for after the session and at the end of the session and move on with Aaron's presentation. But we'll take time to cover some of the Note 4 questions now.

>> Anita Zinzuvadia: Okay. So, one of the Note 4 questions I received was, "Can an item fall under Note 4, regardless of the encryption strength?" Again, the primary -- using the primary function, if the item falls out of -- out of because of Note 4, it does not matter how strong your encryption is. So, the answer to this question is, essentially, yes -- an item can fall out of -- can fall under Note 4, regardless of its encryption strength. The second Note 4 question I received was about the bus-route application that I was talking about. And I really do use a bus-route application to get around town. It's really helpful. [Laughter] So, the mobile application -- "if it's sending and receiving information, does it still qualify for Note 4?" And that was -- The point I was trying to make was that, although it's sending and receiving information, it's really -- its primary function is really to provide you with your transportation information, your bus-route information, and so, even though it is, inherently, doing some communications -- sending information. Obviously, there's got to be, you know, these -- this app is really well-timed because I can go out there and get to a bus, and I know it'll be coming in a couple of minutes. So there's some communication there between some GPS receiver on the bus that is coming to -- that's talking to a server that's getting relayed to my phone. But, again, that communication is really being held within an application for providing you with information about the bus routes. So, Note 4 would apply, even though there is the inherent feature of sending and receiving and storing information. I received some encryption registration questions. One was, "Can I keep my encryption registration from year to year -- my 'R' number?" And as some of you know, when you submit your -- a new "R" number -- when you submit a new encryption registration, you automatically get a new "R" number. Some -- And the

question is whether I can keep my "R" number from year to year. We've said that -- or we are saying now -- that if you want to keep your "R" number from year to year to be constant, you can e-mail us, and we have the ability in SNAP-R to reopen your existing "R" number so you can upload your new Supplement No. 5 if the questions to -- if the answers to your questions have changed in the Supplement 5, so that is an option. And the second part of that question was, "Can I cancel an 'R' number?" There's no formal mechanism for us to cancel an "R" number. And I guess the situation could arise in several different forms -- if the company has folded or you have a Note 4 item and you realize you never needed an encryption registration or you've merged with another company -- those are all examples of where you would no longer need your encryption registration. Again, you can send us an e-mail, and we could make note of it in our records, but that is not a requirement. That is in no way saying that we require you to send us an e-mail to cancel your old "R" number that's not being used. So, the question really was -- the second part of -- or the third part of that question was, "If I file an encryption registration, does that mean I have to file a self-classification report?" And the answer is "no." If you file an encryption registration but you don't make any exports, you don't need to file a self-classification report, or your company no longer exists -- we're not gonna -- we're not gonna look at all encryption registrations and make sure they line up with a self-classification report every year. It's just not something that we do. Okay, so, I have another question -- "Our software product falls under the ECCN of EAR99. However, we add a third-party product of 5D002 ENC. Does our product ECCN change to the more restrictive ECCN?" Well, I guess it depends. If your item is EAR99 because it was Note 4, then you need to look at it -- look at the primary function. If, by adding this 5D002 software to your product, the primary function has changed, then it may not be a Note 4 item anymore. So, this -- it's kind of an open question and really depends on the specific details. Other question was, "Our (b)(3) and (b)(2) items are grandfathered into the -- under the June 2010 rule. We have had no products since, so we have not yet made the registration. For NSA reporting purposes, do we still need to add the 'R' number, which we don't have yet?" The answer is, if your items are grandfathered under the new rule, then you don't need to submit an encryption registration for your items or for products that were under the old rule -- that were classified under the old rule. It's for products since June 25, 2010, where the regulations and the requirement kicked in, where you would need to submit an

encryption registration. So, if you have only grandfathered items that were classified prior to June 25, 2010, there's no encryption registration requirement.

>> Sylvia Jimmison: [Speaking indistinctly]

>> Anita Zinzuvadia: And Sylvia's pointing out, unless, you know, you're changing your product's functionality or encryption functionality or if you have new products after June 25th, then the encryption registration requirement would kick in because you're classifying under the new regulations. Judy?

>> Judith Currie: Good morning. I've got a couple of questions here. The first one concerns car audio/stereo equipment using Bluetooth technology. And there are a number of "get out of encryption free" cards that you could use on this one. The first one is that if it is shipped as an -- shipped separately was the question, and if it's shipped as an audio system, then it would fall under Note 4. But if it were just the Bluetooth adapter for it -- if it were sort of a generic Category 5, Part 1 if it didn't have encryption -- Bluetooth adapter -- then you would need to step back and set -- ask the question -- because then it would be a communications device that would not meet Note 4. So your first question would be, "Is the range more than 30 meters?" Which is the criteria for related control note (i) for wireless PAN equipment. If it is 30 meters or less, you can self-classify as 5A992 -- do not have to worry about registration or (b)(1) reporting. Let's just say, for the sake of hypotheticals, that it exceeded the 30 meters. Then you would look to the (b)(4) paragraph for items that incorporate short-range wireless. The adapter -- the wireless adapter or, for example, an access point or router with wireless technology, meets the technical criteria, but since they are Category 5 items, they cannot be self-classified under 740.17(b)(4) or 742.15(b)(4). So, in other words, if all of those three ways fail, then you're down to a (b)(1) item, either probably -- usually, a mass-marketed (b)(1) item. You submit a registration and do the self-classification. Now, one little more piece about that question is they added, saying, "including cellphone Bluetooth technology." Well, obviously, if it has a cellphone with it, you're automatically into the registration and self-classification because the cellphone's not going to meet the short-range -- any of the short-

range wireless provisions. The second question had to do with the fact that many people are demanding higher and higher security for their networks and, where their networks might have not met the (b)(2)(i)(A) infrastructure criteria in the past, that they're starting to meet them. And the question is, "Are you reviewing the technical levels for items that fall under the infrastructure paragraph of (b)(2)?" And, yes, not only are we -- that is an obligation that you need to do. You need to -- If you're increasing the technical capabilities in terms of encrypted throughput or number of number of simultaneous encrypted tunnels, you need to look at (b)(2) and say, "Does my -- Could my item be described here?" And if so, then you would need to submit a classification request, even if, in the past, before the enhanced capabilities, it would have been a (b)(1) item -- or a (b)(3) item in the past. Thank you.

>> Female Speaker: Sylvia.

>> Sylvia Jimmison: Oh, okay. All right, I have one question, and it's, "Do we need to be applying for licenses for foreign nationals who work in our I.T. support if they are utilizing products that are generally available in the public domain?" The answer is "no." The other half of the question is, "What kinds of questions should we be asking in order to better analyze whether those foreign nationals are utilizing controlled technology?" And the response is, unless the foreign national is from the E:1 country, they're authorized under (b) -- (a)(2) to access U.S. technologies. License Exception ENC allows foreign nationals --

>> Female Speaker: Excuse me, Sylvia. Could you bring the mike closer to you, please? Thank you.

>> Sylvia Jimmison: Okay, License Exception ENC allows employees of U.S. companies to access U.S. technology for -- the release of technology for encryption under paragraph (a)(2). That's the only questions I have. Thanks.

>> Randy Pratt: There were several questions for Mike, but in the interest of keeping the program going, we'll save those for after Aaron and Joe's formal presentations. So, we'll continue with Aaron now. Thank you.

>> Aaron Amundson: All right, so, I'm gonna talk about what's new in Category 5, Part 2 this year. There are basically three new regulatory developments in Category 5, Part 2. [Clears throat] Sorry. First, we published two new rules that deal specifically with Category 5, Part 2. The first is the publicly available rule for encryption software that was published in January 2011, and that rule released from the EAR certain types of publicly available encryption software. I mean, you should all have the pink handout that discusses the publicly available rule that I'm gonna go over in just a couple of minutes. And the second rule that we published is the cryptographic activation rule. That was part of the 2010 Wassenaar amendments to the EAR. That was published in May. And this is what we refer to as our dormant encryption rule or policy, and the rule is really meant to be a codification of our controls on products that have dormant encryption. It's not a new control on these products, and in fact, if anything, I think it is a slight liberalization of our previous dormant encryption policy, which I'll talk about, also, in a minute. And then, the third issue that I'll talk about is the Form I-129 certification requirements for deemed exports. As many of you, I'm sure, know, the Form I-129 is a form that employers have to fill out for certain foreign national visas, and the form now requires employers to certify that they will comply with the deemed export requirements, if applicable. And so, as a result of this, we've gotten a lot of questions about how deemed exports apply specifically to encryption products, and so I'll talk about how the deemed export rules apply to encryption. So, the first thing I'll talk about then, is the publicly available encryption software rule. And the rule removed from the EAR jurisdiction certain types of publicly available encryption software, so it's no longer subject to the EAR. And I think, at first, the rule seems a little counterintuitive in that, in order to treat the software as not subject to the EAR, you have to sort of pretend that it is subject to the EAR and comply with the regulatory requirements, the notification or registration or review requirements, and then you have to treat it as not subject to the EAR. And I think one good way to understand why that is, is, if you look at the way the rule was before and how this rule changed that. So, under the previous rule, publicly available source

code and the corresponding object code remained subject to the EAR -- even though it was publicly available, it remained subject to the EAR, but it was eligible for License Exception TSU once you sent in the e-mail notification with the URL address under TSU. And then, also, in the EAR, there was a note that said, if you're making mass-market software or TSU-eligible software publicly available by positing it on the Internet for free and anonymous download, it did not raise any red flags. And what that meant was that if you're publishing mass-market or TSU-eligible source -- software on the Internet for free and anonymous download and somebody in an embargoed country downloaded the software without your knowledge, it's not a violation of the EAR. And so that's what the old rule said. In this rule, we sort of took it one step further. So, instead of saying it's -- instead of saying it's not subject to the -- it's subject to the EAR but eligible for TSU and available for free and anonymous download, we just said it's not subject to the EAR. So, in other words, the regulatory requirements for the products themselves have not changed. The same products that required a review or a notification or a registration under the old rule continue to require that under the new rule. It's just that the outcome is different. Instead of it being available for free and anonymous download, it's not -- now not subject to the EAR. So, if you take a look at the handout, the pink page, the handout -- there's two types of software that are released from the rule, and the handout provides sort of the elements that you have to meet under each type of software in order to consider it not subject to the EAR. So, the two types of software that are released by the rule is publicly available mass-market software that's had the required notification or classification, and the second type is the publicly available object code when the corresponding source code is eligible for License Exception TSU. And one thing I wanted to point out here, as the handout says, is the rule really only applies to software. It doesn't apply to encryption source code. The rules for the encryption source code are the same as under the previous rule. They're subject to the EAR, but eligible for TSU notification. So this rule -- when we're talking about this rule, it really only applies to software.

>> Randy Pratt: [Speaking indistinctly]

>> Aaron Amundson: Okay. Okay, we got a question that says, "What does 'released from control under the EAR' mean? Does the item revert to EAR99 or 5D992? What is the item's new classification and authorization?" When we say it's released from control under the EAR, it means that it's not subject to the Export Administration Regulations, so it doesn't revert to any ECCN -- it just means it's no ECCN, 'cause it's not controlled under the Export Administration Regulations. Of course, that doesn't mean it's not controlled under OFAC or some other regulatory regime, but it's not controlled under the EAR. There's no requirements to do anything under the EAR. So, if we take the first type of software that's removed -- on the handout -- the publicly available mass-market software that's had the required notification, the handout lists the five elements -- or four elements that are required to make the software no longer subject to the EAR. The first is that it has to meet -- it has to be publicly available. It has to meet the definition of being "publicly available," which is a defined term in the EAR. And typically, when you're talking about encryption, it usually means somebody's -- you're posting it for free on the Internet, for free download. The second one is that it has to be -- it has to meet the mass-market criteria, because the rule is only for mass-market products, so it has to meet the mass market criteria. Next, the manufacturer or exporter has to submit the ERN and get the Encryption Registration Number. Since that's required for the item to be eligible for mass market, it requires the registration. And one thing I wanted to point out about that is, for the (b)(1) items, items under 742.15(b)(1), that also, of course, has the annual self-classification report requirement, and the report would still be required under this rule, even though the product is no longer -- would end up no longer subject to the EAR, but you only have to submit it in the year that you are making the software publicly available. So, if you make the software publicly available this year, you'd only have to report it in your report next year, and you only have to do it that one time. And then, the last element is that the product has to have been -- if the product required a review under 742.15(b)(3), which Anita and Mike went over, it would require a review under this rule before it could be removed from the EAR jurisdiction, so that's the toolkits and chips and those kinds of products. So, two other things to point out about the rule -- as the handout says, the registration requirement is really only required for products that were submitted for a classification after the -- after June 25, 2010. That's because of the grandfathering provisions in 742.15 and 740.17 that products that were submitted for a

classification before that are -- you know, were grandfathered in under the new regulations. And then, one other little subtlety in the rule is that the registration and classification requirements are only -- for mass-market products -- are only for products with symmetric key lengths greater than 64 bits because, if it has symmetric key lengths not exceeding 64 bits, then it can be self-classified - - it doesn't require a registration or classification, so it wouldn't be required under this rule, either. So, that's the first type of software that's released. The second one, I think, is a little easier -- publicly available object code when the corresponding source code is eligible for TSU. And so that one -- under that provision, first, the software and the object code have to be publicly available, as that's defined in the EAR, and then, somebody has to send in -- and, usually, it's the person that wrote the -- drafted the source code, but it could -- I think it could be anybody -- send the e-mail in with the URL address that's required under License Exception TSU. And the notification under TSU is really only required for the source code, not for the object code. So, if the source code and the object code are in different locations, the notification is really -- is only for the source code. And then, in that case, the object code -- once that's done, the object code is no longer subject to the EAR. So, one question that we've gotten since the rule's come out is whether or not we'll issue a classification saying that a particular application is not subject to the EAR. And I think the answer that we've decided on is that we can't issue a CCATS with the ECCN number and a statement that it's not subject to the EAR because if it's not subject to the EAR, we shouldn't be providing an ECCN for it. So, if you want us to confirm that the item is not -- you know, meets these rules and is not subject to the EAR, you have two choices, I think. One, you can submit the classification and ask us to determine whether or not it's subject to the EAR, and if we can determine that, then we can RWA the classification. But in that case, you wouldn't get the ECCN number -- we would just RWA it. And the second option, I think, is, if you want the ECCN number, you can submit the classification and get the classification done, and then you can send an e-mail to the licensing officer and explain why you think it's not subject to the EAR and ask them to confirm that. So, I think those are the two options that you have. All right, so, that's it for the publicly available rule. The next rule that I'm gonna talk about is the cryptographic activation rule. And this was part of the Wassenaar 2010 implementation rule that was published in May. And it -- as I said, it's meant to be a clarification of our dormant encryption policy. It's not a new control, and if anything, it's a

slight liberalization of our controls. So, the rule does two things. First, it adds a new control paragraph under 5A002, 5D002, and 5E002 for the encryption licensing mechanism. And then, the second thing is it adds a decontrol note (j) to 5A002 to decontrol products with dormant encryption. So, the dormant -- the product itself with dormant encryption would fall under, then, 5A992 or 5D992. So, the first thing it does is it adds a new control paragraph to 5A, 5D, and 5E. And the control paragraph basically says that it controls a -- it controls a product that takes another product from being not controlled under the ECCN to being controlled under the ECCN. So, an encryption licensing mechanism takes a product that is not controlled under 5A002, 'cause the encryption is dormant, and activates the encryption and so puts it into a state where it's controlled under 5A002. So, that's sort of the rationale behind the language in the control. And we added it as a separate control paragraph in the ECCN to make it clear that the licensing mechanism is controlled at the same ECCN as the product that it's activating. And there's controls in 5A and 5D, obviously, to account for hardware and software implementations of the license keys. And then we added a -- we also added a 5E002 control. That was really done in order to provide other Wassenaar member the option of controlling license keys as technology. But, we in the U.S. do not control the licensing mechanisms as 5E002 technology. So, even though we added the 5E002 control, we would not control the encryption licensing mechanism as technology. And then, also, I always like to say this when I talk about the cryptographic activation rule, but just to be clear, the cryptographic activation that we're talking about is the mechanism that activates the encryption functionality, specifically, in the product. So, this rule does not apply to a licensing key that just allows you to use software application in general or turn on the software application. We're talking about the mechanism that is specifically activating the encryption functionality in the products. So, the -- And then the -- So, that's the first thing to note the rule does. The second thing it does is it adds a decontrol note (j) to 5A002 for the product with dormant encryption. And it decontrols products where the encryption cannot be used or where it can only be made usable by means of cryptographic activation. So, I think the first one is more difficult to analyze and a lot more fact-specific. "Where the encryption cannot be used" -- that's the first one. And we've said that if it just -- if the encryption is just sitting there and just requires some additional software to work, we would not consider that to be dormant encryption. On the other hand, if the encryption is -- if you're disabling the encryption in a way

that it -- technically, it could not be re-enabled, so you're permanently disabling it in a way that it could not be re-enabled, we would consider that to be not encryption at all, if it's completely disabled in a way that it cannot not be re-enabled. So, that's the first one. The second one, I think, is a little easier to apply, where the -- it can -- the encryption can only be used by means of a cryptographic activation. And the term "cryptographic activation" is defined as a definition in the EAR. And that's where I was saying earlier that I think there's a slight -- this is actually a slight liberalization in our dormant encryption policy. The definition says that it applies to techniques -- any technique that activates the encryption functionality implemented by the manufacturer and uniquely bound to the item or a customer for which the encryption is being activated. So, the slight liberalization is the "or a customer" part, meaning that -- before, we said the activating mechanism that's activating the encryption functionality had to be uniquely bound to the item that it was activating. In other words, it -- the licensing mechanism reads some unique I.D. Number on the device, and it will only work if it reads that unique number, and that way, if I get the licensing mechanism for one product, I can't turn around and use it on a different product that the manufacturer didn't intend. So, the new rule says that, even if it's not bound to the particular item, if it's bound to a particular customer, it would still be considered a licensing mechanism that the product could be considered dormant. So, in other words, if you -- if there's a -- if you come up with a mechanism that binds the licensing mechanism to a customer, like you use a unique customer I.D., and it will only activate the encryption if it reads that unique customer I.D. -- And that way, if the customer has one item, it'll activate just that one, or if they have 50, it'll activate all 50. So, under...the EAR, the way that this is implemented is the dormant encryption product is -- you can self-classify the product under 5A992 or 5D992, 'cause it's part of the decontrol notes. So it would fall under 992, and you could self-classify it. The activation mechanism, as Mike mentioned, is controlled under (b)(3), so 740.17(b)(3) or 742.15(b)(3). So, the activation mechanism would require a review, and that applies even if the product that it's activating is a (b)(1) item. So, if it's activating a (b)(1) or a (b)(3) item, it would fall under -- the activation mechanism falls under (b)(3), and then, of course, if it's activating a (b)(2) item, then the activation mechanism would also fall under (b)(2). So, that's basically how it works under the EAR. And then, the last thing we did with the rule was we added the term "cryptographic activation" to the

definition of "information security." And that was really just to make it clear that activating encryption functionality in a product is part of the information security function that generally falls under Category 5, Part 2. So, that's the cryptographic activation rule. The final issue that I'm gonna talk about is the Form I-129 certification requirements for deemed exports. And as I said, this is a -- the I-129 is a form that employers have to fill out for certain foreign national visas, and it -- the form now requires the employer to certify that -- I think it requires them to certify that either the technology doesn't require a license or it does require a license and they're going to get a license. And so, as a result of this, we've gotten a lot of questions about how deemed exports apply to encryption. And, as Sylvia sort of alluded to earlier, the bottom line is that deemed exports licenses are generally -- for encryption products -- are generally not gonna be required, except for transfers to E:1 nationals, so that's sort of the bottom line. The deemed export license will generally not be required unless you're transferring it to a foreign national -- I mean, an E:1 national. And the reason is because of the combination of the way that exports are defined for encryption products under Section 734.2 and because of the way that we've interpreted License Exception ENC and, specifically, 740.17(a)(2). So, first, if you look at the definition of "export" in 734.2, the definition of "export" says, "For encryption software and source code, look at paragraph (b)(9)." So, if you look at paragraph (b)(9), it says that, for encryption software and source code, an export is either a transfer outside of the U.S. or a transfer to a foreign embassy within the U.S., so it doesn't define an export as a release within the U.S. to a foreign national. So that means that there's no deemed exports for encryption software and source code. So, a transfer of encryption software or source code in the U.S. to a foreign national is not considered an export. For technology -- For 5E002 technology, 734.2 does not have a separate definition for "encryption technology." So, that means that it's defined -- for encryption technology, an export is defined the same way as in the rest of the EAR, meaning that there are deemed -- that a transfer is -- within the U.S. is considered a deemed export. However, we have interpreted Section 740.17(a)(2) of License Exception ENC broadly to apply into most instances of in-country transfers of deemed exports of encryption technology. 740.17(a)(2) is the provision that allows you to export to U.S. subsidiaries, and it also allows you to export to -- allows exports by a U.S. company and its subsidiaries to foreign nationals who are employees, contractors, or interns of the U.S. company. So, of course,

there's no definition of "U.S. company," but we've interpreted that to apply to any company in the U.S. So, that means that any company in the U.S. that -- 740.17(a)(2) allows a company in the U.S. to transfer 5E002 technology to their foreign national employees. So, that's why I said, in most cases, a deemed export license will not be required for encryption products, except to E:1 nationals, because, in most cases, either it won't be considered -- it's not considered an export, or if it is considered an export, it'll be eligible under 740.17(a)(2). And there's a couple other limiting factors to keep in mind. One is that it -- of course, it has to be controlled 5E002 technology, so it has to be development, production, or use technology, and for use technology, it has to be all five or six of the elements, so you're really only talking about 5E002 development or production technology. And it has to be -- your publicly available technology would be not subject to the EAR, so you're really talking about proprietary development or production technology. And another factor, also, is that License Exception ENC now for technology authorizes exports to a much broader range of people than it previously did, so if the technology has been reviewed, if you're talking about the, you know, technology other than the nonstandard cryptography and cryptanalytic and -- I'm forgetting something else. But it's eligible under ENC once it's been reviewed to non-government end users outside of country -- D:1. So, I think that's another factor that would limit the number of deemed exports licenses that we would see for technology. So, the last thing I'll say is that there is guidance on our Website, also, for deemed exports. If you go to the BIS Webpage and the "Encryption" page, there's a "Frequently Asked Questions" link, and one of the frequently asked questions deals with deemed exports, and it's basically a shorter version of what I just talked about. So, with that, I will turn it over to Joe to talk about what's next.

>> Joe Young: Thank you, Aaron. I'm gonna begin with a little not-so-secret secret. Most of you by now should know that Randy is now the acting... chairman for the Bureau for next year. Congratulations to Randy. So, why do I mention this? That's because now we're talking about my assignment for next year. [Laughter] So, one day, and Randy could -- she'll come in here -- "And here's what you need to do on the issue while I'm away." So I'm gonna do my best to make this happen. So, my first assignment is to continue the Wassenaar discussions and make sure that we push for further relaxation on the encryption front. The second one is to do the final rule that we

have published in -- the June rule, last year, to make it final, and then, also, to work on export-control reform -- see how we can take advantage of the activities -- political activities -- to further the encryption export controls. Okay, so, there are two things we can talk about Wassenaar right now. One is the ongoing activity this year, in 2011, and then the activity that we're looking forward to next year. There is a rule that the U.S. submitted to Wassenaar to decontrol components for mass-market stuff. So, the proposal will include, from Category 5, Part 2, controlled components of mass-market products that are not themselves sold or distributed through mass-market channels, so things that are already distributed back on the mass market -- but whose own status is already mass market, but they are things that -- for manufacture, for example -- go to OEM suppliers -- generally, we don't consider mass market, but they actually got going, eventually making the mass-market stuff -- this rule will help you in that direction. Okay. So, the end product must be able to meet the mass-market note. Once it's finished, is the component going to the main product? Now, this rule was, shall we say, well-received, but with significant reservations during the spring meeting on Wassenaar? We are optimistic that it will happen, but we cannot say for sure it will because this is an item that's subject to negotiation. So, we look forward to see it happen, but we'll see what happens. For next year -- Wassenaar next year -- I would remind everybody that we are beginning to collect ideas and notions and proposals for next year. In fact, next week, the ISTAC is meeting here in Washington. The formal TAC is going to start kicking off with ideas and notions for next year's discussions. So, I'm reaching out to the bigger body here that, if you have some ideas of your own, it's time to tell us about it, and we will try to work that into the proposal, if it is something that can be done, so... And Aaron Amundson is the ISTAC DFO, so please submit the ideas to us, and I know Aaron will be eager to hear from you. All right, so, back to the final rule -- So, we know that the June 25 rule that we're working with right now was the interim final rule, with requests for comments. And we received comments from you on this rule. Thank you for -- Thank you. The comment is now being worked on, and we're looking to implement them into the new rule, for -- in terms of the areas of clarity and structure, so that they can fit into the rule. One other thing we are working on, for example, is many of you are using the...for sensitive and less sensitive -- more sensitive users. The -- We're trying to let people know what these users are, you know, so one of the things we would think about is to publish these sensitive and less sensitive users for you,

so that everybody can be on the same page. And more further down the road and one other idea would be that, instead of requiring... which we routinely approve, possibly, in the final rule, to make them ENC-eligible for you, as a way to reduce the burden on us -- also, make it easier for everybody. But these are ideas we're playing with in the final rule. That's why it takes a little time. This final rule is a priority action for me. Like I said, Randy said that, you know, "Joe, next year, we're gonna get this thing done, right?" So I'm looking to get it done perhaps by the end of this year for you -- at least get this circulated to the agencies. Now, the final rule doesn't cover all the comments that you submitted. One of the things -- Some of the comments are more forward-looking, requires more review and discussions, and it doesn't really fit very well into the context of formalizing a previous rule. So, we will work on a new rule to implement your ideas. Now, export-control reform is a work in progress. This plan right now, with most of our stuff -- for example, STA that are being discussed a lot in this meeting doesn't apply to us...is taken out of STA. But under the bigger political context, we're looking at what could be done. And, remember, the rule also had a "call for comments" period in December of last year, and we have collected some ideas from you. These ideas have been digested internally. We are trying to think how they would fit into it, in terms of structure and policy for encryption export control, in the future. So, it's something that we're working on. I would ask you, at this time, if you have ideas or proposals, let's hear from it -- we did collect some from industry associations through our call for comments in last December, and they will be looked at internally. So, here we are. To answer Randy, I look forward to hear from you, and maybe next year, I'll come back and tell you what we accomplished for you. [Laughter] Thank you.

>> Randy Pratt: Okay. All right. So, that concludes the formal presentations that we have today. We did have a -- We do have about 20 minutes to answer additional questions, and we'll start with the ones that were relevant to Mike's presentation, and then move on to those relevant to Aaron's.

>> Michael Pender: So, the first is a question that actually came up in the break, and at first -- I may owe some people an apology, 'cause the first question was, "What is WAPI?" [Laughter] And I just sort of assumed that the people in the room knew, but I shouldn't make that assumption,

and I take full responsibility for that. So, to make it a little clearer, WAPI is a Chinese Wi-Fi standard. It's kind of similar to 802.11 in the United States, but it's different in an important way, and the way in which it's different is that there are parts of the WAPI implementation that have never been released to the public, so they haven't been peer-reviewed. They haven't been studied by other organizations. They haven't gone through the same sort of vetting process that 802.11 did before becoming an adopted standard. And the next question was, "If a product -- If a product is used to monitor employee calls with customers for quality-control purposes, would it be considered surreptitious listening, even if there is a notice that the call is being monitored?" And I think there's two things in this question I'd like to point out. First, when we're talking about monitoring employee calls, at least, in the organization I work for, you know, our computers are monitored. If we're doing something improper -- It's put in our employment contracts that we sign in the beginning that we're aware that we're being monitored. There is disclosures every time we sit down and log in. It's not hidden from us that our activities using our employer's computers are subject to monitoring, so there's no surreptitious element there. We're on notice. And, second, most of these systems have some sort of warning tone or whatever for the person calling into the system. Maybe they have a beep every 30 seconds, or maybe there's a message that, "Your calls may be recorded for quality-control purposes." When you're notifying the person that their call is being recorded, it's not surreptitious. So, it's not a technical question. It's, you know, is the person on notice that they're -- what they're saying is being recorded? And if the answer is "yes," then, no, the surreptitious issues don't come into it. The only crossover area I can see would be if you sold a product, and then the person purchasing the product can simply turn off that warning beep or eliminate the warning notices that otherwise would be given, and you know, that's just not what we see as standard products in this industry. The next question was --

>> Joe Young: You may want to say that we consider WAPI as nonstandard encryption.

>> Michael Pender: Oh, yeah, we consider WAPI as nonstandard encryption, but the reason it's considered nonstandard...

>> Joe Young: By definition, yeah.

>> Michael Pender: ...encryption is because it hasn't been, you know, fully disclosed, in terms of how it works. All right, so, the next question was, "Are 5A980 items considered -- covered under Wassenaar?" The short answer is "no." It's not a Wassenaar control. It's a U.S. control under the Omnibus Crime Control and Safe Streets Act, or the particular sections of that act that apply here are called the Wiretap Act. So, the basis for control is not the -- Well, the basis for our 5A980 and 5D980 controls are, you know, IEEPA, or, alternatively, the Export Administration Act, originally. But the implementation is meant to be consistent with this other act called the Wiretap Act that sets these more stringent restrictions that, you know, we simply can't authorize export of these items in most circumstances. We don't have the flexibility, outside of some narrowly...areas that have to be consistent with that Wiretap Act. So, the different basis of control leads to a lack of flexibility, in terms of being able to change the licensing policy. And this is -- this next question was actually very similar to one I answered a moment ago, and it talks about, "When you call a customer-service group, they say the phone call may be recorded, and does that software fall under surreptitious listening? What about video conferencing or Webinars?" Again, as long as there's a disclosure to the person that their call is being recorded, you can't really claim that it's surreptitious. You're -- You've been informed. I mean, a lot of these -- like, on our computers, there's a check box. You're not even allowed to log into it until you acknowledge that your activities on the system are subject to review by your employer. This is a very common practice in employment contracts. Whenever you're issued pieces of equipment, like BlackBerrys at work, you know, your activities using the device are subject to monitoring. Now, this one -- "Can you self-classify an encryption product originally classified under (b)(2), forensic software, but it is now (b)(3), without another encryption classification request?" So, this is going back to the grandfathering provisions that were discussed earlier by Anita, in particular. And the general rule is that, when something is grandfathered, there's no need for coming in for a new review. I will point out that there's an exception to that rule that deals with this area in particular. If you have a (b)(3) item under the old regulations that's now a (b)(2) item, then there is a requirement to come in for review, but there's never an opportunity for self-classifying these (b)(2) or (b)(3) items. (b)(2) or (b)(3) items -- you know, the self-

classification simply doesn't apply. That's a concept that applies to, you know, certain carve-out areas where the decontrol notes apply or (b)(1) or (b)(4), as Anita mentioned. So, whenever you're seeing something that's likely to be a (b)(2) or (b)(3) product or has already been classified and is a (b)(2) or (b)(3) product, the short answer is, self-classification is never going to allow you to get the outcome that you want. But the -- What I think that we're really asking, though, is, "If I had an item that was (b)(2) before --" excuse me. I'm gonna rephrase that. [Laughter] "It was (b)(2) under the old version of the regulations. It's (b)(3) under the new version of the regulations. Do I need to come in and have another document filed?" And the shortest answer is there's no new review requirement, but it's not a self-classification. It's the normal review process that you would otherwise have to go through for any other new product that is (b)(2) or (b)(3) classified. I hope that's clear. When we start talking about the (b)(2) before and the (b)(3) now, it doesn't path well. But think of it more in terms of, if you've come up with a new product that hasn't been seen before, there's a review requirement. If the product is going to be -- if it's gonna have a (b)(2) or (b)(3) outcome, you can't self-classify it, and that will lead you to the correct conclusion in almost all situations. And if you have a question, just call us. This question -- "You mentioned automated tests. How would you describe automated fix programs?" I think this question actually came in in response to what I was talking about -- the automated penetration testing. So I want to be very clear here that we're not just talking about automated test software that makes sure something is working properly -- we're talking about a very narrow category of software that's designed to evaluate whether or not your system can be compromised by certain types of malware or, you know, malicious software intended to cause damage to your system. So, assuming we're also talking about automated fix programs in the same category, if that automated fix program has some feature that's causing it to go around and evaluate whether or not there are weaknesses in these systems, then I'd say it's gonna turn on the facts of that specific product, and it might very well be considered a penetration testing program. The technical details here kind of obscure what's really going on. Our concern is primarily that someone doesn't take this software and then use it against a network that they don't actually own to cause havoc on somebody else's network. If this automated fix program has that same capability to cause that same kind of denial-of-service attack or other interference with somebody else's network, then we're gonna have the same concerns, in terms of

understanding what the product is and going through the review process, because of the potential to cause harm to somebody else's systems. Now, this one is, "Do you agree that forensic items, under 740.17(b)(2), (b)(3)(iii), et cetera, can be used temp-- for engineers traveling internationally for temporary work internationally?" I think I understand what the question's asking. I believe if it's just, "If an item is authorized under (b)(2) or (b)(3), can you use the TMP License Exception?" And the short answer is, if you have use the ENC License Exception and you want to, that's great. If you can use another license exception and it fits -- you know, you've got to go through the details of whether or not it authorizes that particular transaction. TMP has an area for tools of the trade, where an engineer might take their products with them and then do something, or there's another category there for doing product demonstrations. Think of TMP as separate and distinct from ENC. If it's authorized under TMP, great -- it doesn't matter how it would be handled under ENC. It doesn't matter whether it would be (b)(1) or (b)(2) or (b)(3). It's a separate authorization, it covers separate circumstances, and if you can do it under the TMP License Exception instead of going through the full review process, that's fine -- use the TMP License Exception. But whether or not the TMP License Exception is, you know, possible for temporary work, you've got to read the specific requirements of the TMP License Exception. How long is it gonna be out of the country? Is it gonna be under the person's control? Are they going to be bringing the product back with them at the end of the period? And if the answer is "no" to one of those questions, then, you know, look at ENC or some other authorization. But don't worry about whether it would be (b)(2) or (b)(3) when you're trying to figure out whether some completely different license exception would apply. And the next question would be, "Would TMP be used for 5x980 items?" No. I believe the only license exception that's available for 5x980 items -- anything -- 5A980, 5D980 -- is the GOV License Exception, which authorizes certain government agencies for, you know, official use of some of these products. And then the last question -- "Would test equipment designed to tune and calibrate public-safety radios be considered 740.17(b)(2) items?" And I hate doing this, 'cause it's always like my lawyerly weasel answer, but the short answer is, it depends. [Laughter] And the facts are gonna determine the outcome on that, because some of these items would be maybe 5B002, as a more generic piece of test equipment, and some of them get more into the same encryption functionality and features of P25 or TETRA, where they have to have intimate

knowledge of how the product works in order to test it. And I think we'd really want to better understand the facts about the specific product before we tried to give that answer, 'cause I can think of products that would end up on either side of that dividing line, depending on what features were present.

>> Randy Pratt: So, now we'll turn to questions related to Aaron's presentation. [Feedback whines] Do you have your cellphone on?

>> Aaron Amundson: No, it's not on.

>> Randy Pratt: [Laughing] Okay.

>> Aaron Amundson: Yeah, it's not on. Put it back. It's not on. Let's see. Okay, so, I got several questions related to publicly available rule. The first one is, "Regarding the changed items under 00 -- 5x002 TSU items, can you explain in further detail what types of items are affected? Do operating systems -- for example, Linux-based O.S.s, such as Fedora or Red Hat, still remain controlled under 002, or do they move to EAR99? Are operating systems such as these eligible for exclusion from control under Note 4?" So, an operating system would not fall under Note 4 -- a general-purpose operating system, at least, would not fall under Note 4. Operating systems that are -- I think one thing to point out here is that the term "open source" that's used in -- a lot does not necessarily mean the same thing as "publicly available" as defined in the EAR. I mean, I think they generally mean the same thing, but the term "publicly available" is a specific definition, as a legal definition in the EAR. And so I think that the -- you know, what we would call the open-source versions of Linux and Red Hat could meet the definition of publicly available and could fall under these rules if, you know, the software and source code meet the definition of publicly available and they've sent in the TSU notification. And the question says, "Do they remain controlled under 002, or do they move to EAR99?" And, really, as I said earlier, if it's publicly available, it doesn't fall under EAR99 -- it falls under nothing because it's not under the Export Administration Regulations. There's no rules on -- at least, under the EAR -- for exporting it, so it's

not under EAR99 or any ECCN. The next one is, "If publicly available software is not subject to the EAR, why is a report still required?" And I guess -- the only thing I can say is that the rationale is that the regulatory requirements -- under the previous rules, these items were still subject to the EAR, but available for free and anonymous download, but they still required the registration and reporting requirements, and the rationale with this rule is that we're not really changing the regulatory requirements -- it's just that the outcome is slightly different. So, I agree that it's a little counterintuitive that you have to comply with the regulatory requirements but it's not subject, but that was sort of the rationale behind it. The next one -- "I have a -- If I have TSU open-source software shipping with a 5A002 object code, which is installed on a piece of hardware, does the publicly available software rule apply?" And I think -- I guess, if you're taking TSU-eligible software or source code and you're putting it onto hardware and it's not -- if it's not subject to the EAR, then it's not -- even if you install it onto a piece of hardware, it's not -- it's still not subject to the EAR. The hardware is subject to the EAR if it's -- with -- you know, in the U.S. or meets the de minimis requirements and -- or is other subject to the EAR. But the software itself, even if it's installed onto a piece of hardware, would remain not subject to the EAR.

>> Michael Pender: Actually, can I follow up on that one?

>> Aaron Amundson: Sure.

>> Michael Pender: Someone asked me a similar question during the break earlier. And at one point in the past, when you were sending out a Customs form, you could only put down one ECCN for everything in the box. And maybe you had a laptop and you had some software installed on that laptop, and you had to pick one ECCN that applied to the system as a whole. So, you've got this TSU-eligible software, and under the old regulations, it was 5D002. And you install it on this laptop. And now, the laptop -- you may self-classify it as 5A002. It actually makes sense now to take a step back from looking at what you were forced to do under the old system and look at what you can do now. So, if I want to go off and buy a laptop from a mass manufacturer here in the U.S., you know, they'll have the -- they'll have a bill that they'll send me or an invoice that'll have

the laptop listed, and it'll have the software that's installed and the laptop listed as a separate item. And if you take that sort of approach with exporting items under AES now, you know, the laptop is probably EAR99 or 4A992. The software -- you can list it on the invoice, but as Aaron said, it's not subject to the EAR anymore, so don't worry about it changing the classification of the laptop. Look at what's going in the package and how are those items controlled individually? You're not longer constrained to picking one ECCN for the entire thing. You know, the only controlled item in that example now is that most 4A992, and it leads to a more favorable outcome for export and for the control provisions that apply.

>> Aaron Amundson: Yeah, and I got a question about -- specifically, about the laptop, so -- that Mike just answered. So, that's good. We're being efficient.

>> Michael Pender: [Chuckles]

>> Aaron Amundson: Please provide examples of source code that meet the definition of 'publicly available' and does not meet the definition." And I think this is what this is asking is, if something that meets the definition of "publicly available" but doesn't meet the rule -- publicly available rule in the handout, and I think the only time that publicly available -- if you have source code that is publicly available that would not fall under TSU is if you don't send in the e-mail notification under TSU. But, again, that's just a -- the e-mail notification is really just -- you send an e-mail to -- with the URL address, and that's really all -- and that's all you need. And so I think that is -- if I'm misunderstanding the question, you can come up and we can talk about it some more. The last question on publicly available -- it says, "If you have both -- If you have software object code and you have the encryption registration, can it become publicly available, not subject to the EAR before you provide the self-classification report to BIS?" And the answer to that is "yes." It becomes -- as long as you comply with the requirements, it becomes not subject to the EAR. Then you have to submit your self-classification report and, I guess -- I mean, I guess, if you don't file the self-classification report, we would say it's -- it is -- you know, doesn't follow -- it doesn't comply with the rule, so it would be subject to the EAR. But, as long as you file -- as long as you do file

the self-classification report, it's okay. You don't have to wait to file that before you can make it not subject to the EAR. And then I got two more questions -- one on deemed exports and one on dormant encryption. So, the one on dormant encryption says, "To be clear, dormant encryption cannot be applied for software and activation codes in general, even though the activation code actually defines the level of encryption in the software -- can you elaborate a bit on the software -- on software -- on the applicability of software activation codes in general?" And I think the dormant encryption rule can apply. It would certainly apply to software activation mechanisms, and it would even apply to the activation code. I think what they're -- when they're saying "activation code," there are some products where you just need -- you just need to type in a series of numbers, and that activates the encryption functionality. And I guess I agree that it's somewhat of a stretch to say that that falls under -- that that is controlled as software. But we have -- we do have -- controlled those as a software activation mechanism. So, if it's a hardware implementation, like a card or a USB dongle or a software that activates the encryption functionality, as long as it meets that definition of "cryptographic activation," then it could be -- it could fall under that -- under the cryptographic activation technique in the dormant encryption rule. And then, the last question I got was on deemed exports. "If encryption software is bought from a vendor and only used for business purposes and a foreign national is using it, is there a deemed export issue?" And in that case, there would not be a deemed export issue for encryption because the deemed export rules don't apply to software or source code. So, just allowing a foreign national in the U.S. to use software or to have access to the software itself would not -- is not considered an export at all for encryption items, so there wouldn't be any deemed export issues with that. "If a company buys all of its software from vendors with built-in encryption, would there be any deemed export issues?" And there, there would not -- again, there would not be any deemed export issues, as far as letting foreign nationals use the software. Even the technology -- the only time the deemed export rules would come into play would be if you were transferring technology, so... But even just the technology on how to use the software would generally -- is not gonna really raise deemed export issues because the technology for just how to operate the software is probably gonna be EAR99, or, if it's not, it would fall under 740.17(a)(2) if you're giving it to a foreign national in the U.S.

working for your company. So, those kinds of issues and scenarios are generally not gonna raise deemed export issues.

>> Randy Pratt: Okay, go ahead.

>> Michael Pender: I got one more question, which is, "Is there a category for weaponized applications, such as Stuxnet?" And really, at the point where I see the word "weaponized" in the description... [Laughter] ...my first response is, "We file a CJ and we have the State Department determine whether or not they want to control it in the U.S. on that list, because any tools that are designed to destruct or destroy communications equipment or someone else's computers would likely be controlled by them. There's not a lot of legitimate commercial use for such products.

>> Randy Pratt: All right. Sylvia, do you have just a couple more?

>> Sylvia Jimmison: Yeah, sure.

>> Randy Pratt: And then -- Go ahead, and then we'll wrap up.

>> Sylvia Jimmison: Okay, one of the -- one of my questions is, "When I submit a classification request with Supplement 6 information, the item's..."

>> Judith Currie: Just speak...

>> Sylvia Jimmison: "...the Supplement 6 information, the item's open source encryption, do I list all the algorithms used in open source or just algorithms used in my product?" I would just use the algorithms you're using in your product and describe how you're using them -- what functions are they performing for you? -- not list all of the open source algorithms. The second question is, "In various discussion, it is mentioned that a low-level encryption is 56 bits. In other discussion, it's mentioned that it's 64 bits. What's the difference?" And the mass-market review, I guess, threshold

is 64 bits or greater when we start to review. Non-mass-marketed items are generally under the 56-bit purview. That's all I have to say.

>> Judith Currie: Okay. Do you want me to do these two or...

>> Randy Pratt: Sure. [Laughing] Two more, and then we'll wrap up. Go ahead.

>> Judith Currie: Okay. Quickly, someone wanted to...know why, often, regular operating -- mass-market operating systems, such as Windows or a non-open source version of Linux or whatever would be 5D992, whereas the usually more restrictive, embedded version of that software would be 002. The -- You really have to look at what's going on with embedded operating systems. Normally, what they do is allow you to choose what pieces of that operating system you want, and you create a flash of software that you put on a device. The reason Windows or non-open source Linux would be 992 is that it's mass-marketed. That flash that you created is generally not something you can go mass-market. Now, once you put that flash on a device and you have a new product, that product could be mass-marketed. It often would be a Note 4 item, 'cause it would often be a device that would not have, as one of its primary purposes, any of the characteristics in Note 4, so that you could just say it's not even Category 5, Part 2, even though it has that operating system on it. But that little piece of operating system you create with the embedded version, like embedded XP or embedded CE or embedded Linux is generally not mass-marketed, so it stays at a 002 level. The other was a question about, with respect to something like credit-card scanners and having them manufactured abroad -- what do -- how do you have to worry about the technology? If the technology is really, really limited to something like the credit-card scanning, it would be 5E992 and following the 5A992 under the related control note for the scanners. If, on the other hand, it's sort of general-purpose encryption technology that just happens to be being used in that way, then you'll have to look at it as 5E002. If ENC...to U.S. subsidiaries or (a)(1) to (b)(3)(iii) countries didn't apply, then you would look to whether that technology could be exported under the new technology provisions of ENC. And if none of that worked, then you would be subject to a license. But in most cases, if you're exporting technology for something as limited as financial --

U.S. Department of Commerce
Bureau of Industry and Security
Update 2011 Conference on Export Controls and Policy

credit-card scanners, you would be at 5E992 technology, and you wouldn't have a -- it would be NLR.

>> Randy Pratt: Okay. Well, with that, I'm sorry we didn't get to quite all of the questions, but, again, we do have our round tables from 1:00 to 3:00 for those of you who can attend, and we'll be expecting additional questions on the specific presentations there. We do have our contact information on the screen, and we invite you to call us anytime with your questions. And, again, thank you very much for enduring our Encryption Workshop. [Laughter] Thanks. [Applause]