

Encryption Workshop Update 2011 (Part 1)

July 21, 2011

>> Randy Pratt: Thank you. Well, welcome to the Information Technology Control Division's Third Annual Update Encryption Workshop. We have done this same format for a couple of years, and we do appreciate everybody -- so many people staying for the third day of the Update Conference in order to attend our workshop. We -- the entire division -- is here on the podium, and it will be a measure of our cohesiveness if we can avoid knocking each other off the dais. We have Aaron Amundson, Michael Pender, Joe Young, Anita Zinzuvadia, Sylvia Jimmison, and Judith Currie. And I wanted to note, as well, before I forget, that, after the workshop today and after lunch, from 1:00 to 3:00, we will have a round-table session on encryption in the Lafayette Room downstairs. And we have an entire room of several tables to ourselves, and we all plan to be there and would be happy to talk to you about specific questions that involve your products or your companies that we aren't able to address this morning. Now, this year, we don't have a major rule to discuss, like we did last year, but we do have a number of issues that we would like to discuss with you. The Update does give us an opportunity to review the trends that we're seeing and the issues that are raised frequently and to put those together, and so it's a useful exercise for us to consider what we need to address and, in addition, of course, it's always a very nice opportunity to see familiar faces or to put faces with names or voices or products that we have engaged on in the past year. Now, we have, as far as schedule this morning... [Computer beeps] Whoops. ...we have our first session with Aaron and -- I'm sorry -- with Anita and Mike to discuss the implementation of the June 25, 2010, rule that was big news last year. And we do have three handouts that you should have gotten a copy of as you came in, and we will refer to those when appropriate in the presentations. Then, we plan to take a coffee break at about 10:30 and then come back and have some questions and answers for 15 minutes or so on that first presentation. Then we'll come back, and we'll talk about what's new with Aaron and then what's next with Joe Young. And then we'll have another opportunity for questions and answers. And then, again, obviously, after the session or particularly in the round tables this afternoon, we'll have time to answer more specific questions. So, with that, I'd like to turn the podium over to Aaron -- to Anita... Excuse me.

I'm getting them mixed up. ...to start out the presentation on the implementation of the 2010 rule.
Thank you.

>> Anita Zinzuvadia: All right. Thank you, Randy. So, as Randy said, I'm going to talk about the implementation of the June 25th rule -- June 25, 2010, so it's been a little bit over a year, and we've all become very familiar with the encryption -- the new encryption rule and have implemented it into our export-control systems, are loving it, and it's working smoothly, right? [Light laughter] That's what we like to hear, anyway. Well, a large component of the June 25th rule allowed you to self-classify items. However, we did maintain the review requirement on certain types of items. Those are items that are classified under paragraph (b)(2) -- 740.17, paragraph (b)(2) and (b)(3) of License Exception ENC -- and the mass-market provision, 742.15, paragraph (b)(3). The (b)(2) items, just as a review, include items such as network infrastructure, source code, items designed for government end use, penetration testing tools, public-safety radios, cryptanalytic tools, encryption technology, nonstandard encryption technology, and Open Cryptographic Interface. Generally, the old (b)(2) items are still the (b)(2) items from the previous rule to the new rule. Mike will go into some of the subtle differences between the previous (b)(2) items, such as digital forensics, which have moved to paragraph (b)(3). At a minimum, (b)(2) items still require the license to government end users outside of the Supplement 3 countries. (b)(2) items are not mass-market items. And reporting requirement -- we've maintained the reporting requirement for most (b)(2) -- for all (b)(2) items. In addition, we also have a reporting requirement for digital forensics tools that are described in paragraph (b)(3) of License Exception ENC. Also, other items described in License Exception ENC include encryption components. We're talking about chips, electronic assemblies, crypto libraries, software development kits, nonstandard tech -- or nonstandard encryption items, whereas the corresponding nonstandard technology is controlled in (b)(2), the digital forensics, and crypto-enabling items, which Aaron will talk about in greater detail. There was some loosening in the 5E002 technology controls under paragraph (b)(2) from the old to the new regulations on June 25th. 5E002 was loosened so that it could go to all but the D:1 -- Group D:1 countries. So this opened up countries such as India, South Korea, and Taiwan to receive 5E002 technology without a license after a review was completed of the technology. And as I

mentioned, self-classification was a large component of the new rule -- self-classification with an encryption regulation. This allowed self-classification after you submitted your company registration, your one-time company registration, and allowed you to basically self-classify items that were described under paragraph (b)(1). Now, what is (b)(1)? What are (b)(1) items under License Exception ENC in Mass Market? They're essentially those items that are not described in paragraph (b)(2) and (b)(3) or (b)(4). I went through our SNAP-R system and ran some numbers, just to see what type of -- how many reviews we were seeing for (b)(1), (b)(2), and (b)(3) items. So, so far this year, in -- since January 2011, we have License Exception ENC paragraph (b)(1) -- almost 470 items, individual items, have been closed out as (b)(1) under License Exception ENC. The corresponding number for Mass Market is 230. For (b)(2) items, License Exception ENC, we've seen about 400 -- I'm sorry -- 350 (b)(2) items that we've closed out. And License Exception ENC (b)(3) items -- about 220, and the corresponding number for Mass Market is about 30. So, add all those numbers up, and we've been keeping busy. So, the self-classification is also available for items without an encryption registration, without doing your company registration. As indicated on this slide, we -- that could include items under paragraph (b)(4), short-range wireless encryption items, items with weak encryption -- we'll cull those items under the 56, 512, 112 key-linked thresholds, authentication only items that are described in the related control notes under 5A002, and the wonderful Note 4 items. Those items can be self-classified without an encryption registration. As the numbers indicated, we continue to receive a large number of (b)(1) items -- items that could be self-classified. So, to give you some insight in what happens on our side of the house when we receive a review, I'll go through some of the procedures that happen when we receive a Commodity Classification. Usually, they're assigned to one of us, and the first thing we look at when we receive a Commodity Classification is, what are you asking for? What is the request for? Are you making it clear that this is a request to confirm it's a Note 4 item or to confirm it's decontrolled under Note -- under the related control notes of 5A002? Is it a (b)(1), (b)(2), (b)(3), or (b)(4) item? That can quickly give us an assessment of what technical parameters we should be looking at and what things we should be looking at when looking through your review. So, when we make the assessment, we're also looking through the documents that you've submitted in SNAP-R. Obviously, if there's no documents submitted, we communicate to you through

SNAP-R to obtain those documents. And if, at that point, we have enough information to make our assessment, we can take several actions. But before I get to that, (b)(1) items -- we've said that (b)(1) items do not require the Supplement No. 6. However, when making our technical review, if we feel like that we need more information, we can request that you complete the Supplement 6 in order for us to fully understand your product and to confirm that it's a (b)(1) item. But once we've obtained the documents from you and we can make our technical assessment, we can refer the case, if we see that it's (b)(2) or (b)(3) items -- those items that I described the previous slide that still require a review -- we refer those to NSA. We give them a 20-day window to provide us with their recommendation. So, in our referral, we give them a rundown of what we think it is. We can put in some discussion notes if we like, refer it out to NSA, give them that 20-day window, and hopefully, they'll respond to us within that 20-day window. If not, we do have the ability to pull it back after the 20-day window has expired. We usually send them a note letting them know that, "This case is past the 20-day window. We need to get this closed out accordingly," and if there's any outstanding issues, then we do deal with them at that point. But if it's a (b)(1) item, those items don't need to be referred out to NSA or if it's a Note 4 item or an item that's described under one of the decontrols. We can make a unilateral decision and close out the case without a referral to NSA. And obviously, these cases move through the system a little bit faster because there's no referral required to NSA. (b)(1) -- So, this shows you that (b)(1) items -- items described under paragraph (b)(1) don't actually get seen by NSA. We're closing those out on our own. NSA does, however, receive your self-classification report, which includes always your (b)(1) items. And I stood up here last year, saying the same thing, and I'll say it again... [Laughter] ...the self-classification report -- unfortunately named because, although you submit a classification to BIS, the self-classification report is still required, so our plan, or our intent is to change it to call it a (b)(1) report to more accurately describe that. All your (b)(1) items should be reported to NSA -- or it should be reported to us. And it makes sense in that NSA's not seeing any of the self-classification -- or any of the (b)(1) items. They only see it when you submit your self-classification report. So, (b)(1) items are closed out using some standard close-out language. And we all -- And we usually refer to the fact that -- or as a reminder in our closeout language to (b)(1) items that you need to submit your Encryption Registration Number in order to export under

paragraph (b)(1). But if we notice that you do already have an Encryption Registration Number on file, we'll exclude that language from the closeout. And as a reminder, submissions for (b)(2) and (b)(3) items -- remember to include your Encryption Registration Number, your "R" number, in the "Additional Information" field, because we will not close out a (b)(2) or (b)(3) item without an encryption registration on file. So, if you can point that out to us up front -- it's actually a requirement and you're instructed to do so by the regulations -- to include your "R" number in your "Additional Information" field for reviews of (b)(2) and (b)(3) items. I'll add that it's very helpful for you to do it on (b)(1) items, as well, that you do submit to us for review. And the encryption registration -- again, that's the company registration. Once you submit your registration, you receive an "R" number, and, again, the encryption registration, your one-time company registration, is required for (b)(1), (b)(2), and (b)(3) items, along with Mass Market (b)(1) and (b)(3) items. And what we ask for in the encryption registration is a Supplement No. 5 -- it's seven questions. Point of Contact -- this is usually someone that, if we have questions further down the line about your encryption registration, we want to be able to pick up the phone or e-mail the person who is listed in the "Point of Contact." Second thing is a company overview. The third question is, "What's your company technology?" Fourth is whether you export nonstandard crypto items. The fifth question is, "Will you be exporting source code?" The sixth question is whether you're incorporating non-U.S. encryption components. And the last question is if your items are manufactured out of the U.S. So it's not too difficult to complete the encryption registration, and usually, the answers that we see are, "yes," "no." If there's further explanation, you can provide it. Common encryption registration mistakes that we've been seeing is that some will use the old Supplement 5 rather than the new Supplement 5. The old Supplement 5, if you remember, was an encryption checklist for your -- for products. That's not required -- or that's the old Supplement 5. We're using the new Supplement 5, which has the seven questions that I just went over. Or, sometimes, you -- exporters are not submitting any Supplement 5, and they're submitting product documents or a company overview -- something very general, which doesn't give us any of the answers to the Supplement 5 -- to the Supplement 5. Also, we've seen that some exporters include their encryption registration Supplement 5 within a Commodity Classification. Submitting your encryption registration Supplement 5 in a Commodity Classification will not result in an "R"

number being assigned to you. If you notice, in SNAP-R, there's different work items that you can choose. In order to do an encryption registration, you'd have to go through the encryption registration work item and not the Commodity Classification work item. Also, we've been seeing encryption registrations for products -- again, the encryption registration is a company registration and is not required for each individual product or updates to products or when you have new products. We've also seen many encryption registrations for companies that may have only Note 4 items. Note 4 items, as I'll discuss, are -- may -- are not controlled under Category 5, Part 2, and do not require an encryption registration. And, again, re-emphasize, we're also seeing that (b)(2), (b)(3) classifications submitted to BIS do not have the Encryption Registration Number listed in the "Additional Information" field. So, so far, we've received about 1,200 encryption registrations. This is including duplicates. The Office of Technology Evaluation predicted about 700 encryption registrations as a result of their encryption survey last year. And what we're -- The trend that we're seeing is that most of the new encryption registrations that are coming in are from mobile app developers. Judy even ventured to guess that a third of them are probably coming from mobile app developers. Also, part of the Note -- Also, part of the June 25th rule was Note 4. Products that were previously ancillary are now Note 4, and this gave us the primary function assessment. It allows us to focus on the primary function of our product to determine whether it's still classified under Category 5, Part 2. Note 4 overrides all other reasons for control, meaning if your item is -- fits Note 4, there is no reason to look anywhere else in Category 5, Part 2. You're out of Category 5, Part 2. And your ECCN may fall to any other category on the CCL or EAR99 if it does not fall to any of the others. The next place to look, if your item does not fit Note 4, is if it's a decontrol -- one of the decontrols under 5A002. So, these include items such as smart cards, smart card readers, software and equipment for money transactions and banking use, client wireless devices customized for civil industry, wireless personal area network, and dormant crypto. These items can be self-classified as 5A992 or 5D992 without the registration. And Aaron will be further discussing the dormant crypto. For Note 4, there are some considerations that we take into account. We've seen so -- We've seen several items come in and try to determine whether they're Note 4, and we've come up with some considerations that we use or some tools and techniques that we use to determine whether an item is Note 4 or not. These aren't in the regulations, but, generally, the

concept that we use -- the concept of general purpose, versus application-specific. And it's more likely that an application-specific product may meet Note 4 than a product that is more of a general application, that can be configured for a specific application. And what I mean by this is application-specific products -- their primary function may be farther removed from one of the four primary functions identified in Note 4, whereas a general application or a general-purpose tool may have a primary function more closely linked to one of the four primary functions identified in Note 4. So, the best way to talk about this is probably to use examples. Say we have a general-purpose handheld computer, versus a handheld computer with a barcode scanner for inventory-management systems. Now, the general-purpose handheld computer -- we could say that the primary function is being a computer. And as the -- as Note 4 says, computers are still remain in Category 5, Part 2. However, with the application-specific or application-specific barcode reader designed for inventory management is more designed -- its primary function we can characterize as inventory management and less than a general computer. So, in that way, we see that the more application-specific item's primary function is not one of the four that is identified in Note 4. Another example -- a software development kit that can be used for making mobile apps -- so that's pretty much not something that's gonna fall under Note 4. Primary function is a little bit of all of those -- of all the things identified in Note 4 -- information security, sending, receiving, and storing, and, also, networking. However, if we make an application from that software development kit -- let's say it's an application that tracks your bus route -- that application loaded on a mobile app -- on a mobile phone could be identified as a Note 4 item. So, there's that concept of general purpose versus application-specific that we've used to assess whether an item is Note 4 or not. Also, you could be adding functions to a Note 4 item. Say you had a Note 4 printer/copier. That's pretty much a Note 4 item. Primary function is printing/copying -- not one of the four identified in Note 4. But let's say you add the functionality of faxing. Well, that added functionality -- that third primary function pulls it back into Category 5, Part 2, because the fax capability's mostly used for sending, receiving, and storing. So that's an example of an item that was Note 4 before that could come back into Category 5 because you've added another primary function. So, we'll look to the yellow handout in our packet. And we'll go to this funnel on the back of the page. Does everyone have a -- Does everyone have a handout? If you do not, raise your hand, and we'll distribute them to you. So,

when we say "primary function," we're talking about, for what purpose would someone buy your product? How does your marketing or advertising describe your product? What is the primary function? So, your primary function -- once you've identified it, you can send it down the funnel. If it gets caught under any one of the primary -- four primary functions identified, it stays in Category 5, Part 2. Okay, so, if it's not information security, not a computer, not sending, receiving, storing, and not networking, then you can go to the next step. Now, I'd like to make a note about this "sending, receiving, and storing" bit. We understand that sending, receiving, and storing, which I will call "short communication," so I don't have to repeat all of that mouthful every time -- communications can be an inherent function of a product or of your item. However, it may be in support of a main function. So, we make -- we do make some exclusions within the Note, which say, "except for in support of entertainment, mass commercial broadcasts, DRM, and medical records." However, let's say you have a mobile app -- let's take our bus-route app that we have on our mobile phone. Let's say it allows you to -- it communicates. Essentially, your application is communicating information to you. It's doing some sending, receiving, and storing of information. However, that's not the primary function or the main function. That communication is really in support of giving you your bus-route information. So, if your product is a software application for a mobile phone, it -- you don't include communications as a primary function unless the application allows you to do the direct communications -- for example, if it's an e-mail application or an SMS application. Those are -- the primary function would be sending, receiving, and storing. But in our bus-route application, it's really in support of the primary function. So, the last little bit of our Note 4 assessment says that the encryption must support your primary function. And we were talking about -- When we were going through these slides, Joe came up with an example of the "Get Smart" shoe phone. [Laughter] I don't know if you guys ever saw that show with Maxwell Smart and Agent 99, remade into a movie more recently. So, if we use the shoe as an example of something that we throw down this funnel, well, a shoe, to me, the primary function is to be fashionable, but... [Laughter] ...some may use it for other functions. They may use it to protect their feet, okay? So, let's say this -- our shoe phone -- also uses encryption to support the phone calls that it makes. So, the primary function is to be fashionable or to protect your feet. Does the encryption support that primary function? No. So, you have an item

there -- your "Get Smart" shoe phone would not fall into the world of Note 4 items because your encryption does not support the primary function of protecting your feet. So, that's one example. So, once it does fall through the funnel of Note 4 items, then you're out. You're out of Category 5, Part 2, and you don't need to talk to us. [Laughter] The back of the slide -- or the back of the handout includes several more examples of items that we do not consider Note 4. If you look through this list, you'll see that the primary function of these items falls mostly to one of the four primary functions that's identified in Note 4. And you can add the Maxwell Smart "Get Smart" shoe phone to this list. I'm going to now hand the podium over to Michael Pender, who will discuss the new product descriptions under paragraph (b)(2) and (b)(3).

>> Michael Pender: Thank you, Anita. Oh. That's very dark. All right, so, before I start getting into what's new, I'm actually gonna take you back what's probably gonna seem like an awful long time to the old version of (b)(2) that we used to have, and specifically, for anyone who doesn't have memorized 740.17(b)(2)(iii) from the, you know, pre-2010 version -- yes, that includes me -- it used to say, "encryption software, commodities, or components therefor that have been designed, modified, adapted or customized for government end-users, for government end use," and I'm gonna skip a little bit here -- followed by examples of what we considered controlled products, and it included emergency-response communications, the Security Operations Center, the Network Operations Center, command and infrastructure, public-safety radio, digital forensics, and computer forensics. Anyway, it was exemplary language. It was under this government end-use or end-users' structure, and I can't even count the number of phone calls I've had and the number of hours spent explaining why we considered some of these things to be government end use. And I'm not gonna try and justify those conversations at this point, but I will say that the new version's a lot clearer, and hopefully, you'll agree with that, as soon as we start digging into this in just a moment. So, the new 740.17(b)(2)(i)(F) is this network penetration or testing tools. And for people who aren't familiar with exactly what these products are and what they do, these are tools that have been added to (b)(2) because they have an offensive capability. And by that, I mean they're sort of a double-edged sword. Their purpose is to conduct automated tests of a network for vulnerabilities that can be exploited to insert a virus, a worm, or a malicious code. Now, generally, the primary

legitimate use for these tools is when someone goes and they want to check out their own network. They're responsible for making sure that their company doesn't get infiltrated from the outside. So they're looking for weaknesses that can be exploited by a hacker. Unfortunately, the same tools are just as useful in the hands of the hacker to exploit that same network and insert their code. So, some of these tools in this category actually go a step further, and they breach the firewall, and they install a payload of malicious code in the targeted system. Now, for people who'd like me to kind of bring that down from 60,000 feet to something a little bit closer to earth, what we're talking about is the analogous to -- you know, if the firewall is the fence around your house, are they just going up and checking whether there's a fence there, or are they actually, you know, trying to go up to your front door and knock, and no one answers, and they open the front door, and they stick their head inside and look around? It's going beyond merely observing what's there and going to the level of, you know, are you vulnerable to this kind of attack that can be launched against your network? And that's one of the reasons that these are specifically identified as something controlled under (b)(2) as a restricted commodity. Also, under (b)(2) is the public-safety and first-responder radio. This has actually been broken out into a second paragraph now. So, it's 740.17(b)(2)(i) paragraph "G." And the reason is just to make it clear that, whether it's a P25 radio or a TETRA radio or an emergency-response system for the police or fire or ambulance, this is a controlled item, and it's controlled in this area. And we don't have to get into whether ambulance use is government use -- under the old structure. It's hopefully considerably clearer. And this brings us to 740.17(b)(3)(iii). So, we're actually out -- we're actually talking now about something that used to be controlled under (b)(2) that has been relaxed down to (b)(3) with the new system. And this is the packet inspection and forensics tools. Now, previously, this was described under (b)(2) as "digital forensics, computer forensics," and it was under that government end-use structure again. Now, I want to emphasize that, even though this is a (b)(3) area, semiannual reports are not required for most items in (b)(3), but they are still required for these items in (b)(3)(iii). So it's kind of an exception that we still care and we still want to receive the reports on these for the semiannual sales. Now, again, this includes network analysis, packet inspection, and forensics tools, and if the network penetration tools are the swords of the I.T. people, then these are really the shields, because they're primarily defensive in use. Administrators install these tools to

monitor employee conduct on their own network, and what they're looking for is illegal activity, violations of systems-usage policies. I used to work for a company that found out that one of their employees was using a government -- not government -- a company-issued computer to host illegal files and trade porn on the machine. [Light laughter] And, you know, this is the sort of thing that companies -- responsible companies have an obligation to police their own systems for and make sure employees aren't abusing the privileges they've been given. In fact, under some legal requirements, like HIPAA or Sarbanes-Oxley, there might even be a legal requirement to conduct some self-monitoring of your systems. So the intent is not necessarily to capture everything that's gonna be put into that kind of a use. In talking to Anita about this, one of the things she asked me to point out is there very specific language in there -- if you study this paragraph -- and it talks about whether you're doing automated remediation. And the difference is, if you are gathering information about how your employees are using the network and you're looking -- you're having a human being look at that and say, "Okay, you know, why are they doing this strange thing? Why is this traffic happening late at night with these large files moving back and forth?" It's different than having this automated system set up in place that's proactively trying to detect improper behavior or profile that behavior and make changes in the network and to policies in response. Since it's not gonna apply to everyone in the room, I don't really want to dig into it in too great of detail, but I would encourage you not to read past the specific language that's been put in there to limit how broad this category goes, 'cause it's not intended to capture everything that you would defensively use for properly policing your own network. Now...who's got their blue sheets? This is the handout. We're looking at the side of it that says "communications intercepting devices." Does anyone not have their blue sheet? Okay. Looks like we're good. Well, there have been a lot of questions in this last year about how to distinguish between what's in 740.17(b)(3)(iii), which is the computer tools for network forensics or computer forensics, the (b)(2), (c)(1) tools for government end use, and the 742.13 5A980 tools or 5D980 tools for surreptitious listening. And it's because the relationship between these, I think, maybe wasn't made clear to people, in terms of what we control in the various levels of restriction. So this is our iceberg diagram again. And what you'll notice in looking at this iceberg is there's no water. [Chuckles] This is the part of the iceberg that's all above the water and that we care about all of these, but to varying degrees. So, the very tip of the

iceberg is the surreptitious listening items. Beneath that is the restricted items that aren't controlled as tightly. And then, beneath that is the unrestricted items that maybe have more restrictions -- more requirements in terms of compliance than some of the other (b)(3) items, but it's not as sensitive as either the surreptitious listening or the products that are restricted for sale to government. So, starting with the (b)(3)(iii) parts, the stuff in the very bottom, the data forensics and network forensics. So, these are the commodities and software that provide or perform vulnerability analysis, network forensics, and computer forensics functions, and includes items that statistically profile user behavior or that capture and analyze digital forensic behavior for law-enforcement purposes. But it's not specifically being done by, like, law enforcement or, you know, for the use of a law-enforcement agency. An example would be a computer -- a company purchases a system, and they install it, and they're monitoring their employee behavior for illegal activity. Like I mentioned earlier, I once worked with a company where they had to, you know, arrest the person and confiscate their computer and walk them out. It's just the nature of large enterprises that, every so often, you're gonna have an employee, and you've got to keep tabs on what they're doing, and you find that you may need to preserve that evidence yourself in case you have to fire the employee and defend your company in a lawsuit if the employee's arguing that they were being fired for illegitimate reasons. Just because the information is being preserved for use later and could possibly be used in a court of law does not mean that we consider it a government end use. Now, I'm gonna compare that against the (b)(2) items and, specifically, what I have in mind here is what we call "lawful intercept gateway products." So, the general structure there is encryption software, commodities, and components that have been designed, modified, or customized for government end uses. And when I talk about "lawful intercept gateways," I'm talking about an appliance that you add to a telecommunications network, and it's for law-enforcement personnel that, when they get a court-ordered wiretap order from a -- you know, from a FISA court or something, they can go to the telecommunications company and say, "All right, we need to execute a wiretap on this telephone number. We need to record this information." It's not the actual box that the law-enforcement personnel take with them. It's kind of a bridge between their device that does the actual wiretap and the telecommunications switch that just passes phone calls back and forth to everyone. So, it's a box that exists in that switch system for the

government's use, and it's sold specifically for the government's use, but it's not the actual wiretap appliance. And I do want to emphasize here that merely being CALEA-compliant -- like, having a CALEA-compliant communications switch does not result in a classification in (b)(2) in this area. So, if you're worried because you're involved in a telecommunications company and you say, "Well, I've got a -- I'm required by law to comply with CALEA. Does that mean all of my products are (b)(2)?" And I've had that question a couple of times. The short answer is "no," but we probably do need to drill down and understand the product very well. And then, lastly, this includes cryptanalytic commodities and software. And it may seem odd to put cryptanalytic in this part of the discussion, but the rationale is that, sometimes, people will intercept and then later analyze and decrypt that content, and this is sometimes done with telephone calls, where people are using encrypted communications and there's a law-enforcement interest in obtaining the content of that information. So, any devices that are cryptanalytic, that are trying to brute-force decode what's being sent back and forth are (b)(2), as well. And we would control that, you know, whether or not the government end use was involved. The cryptanalytic commodities are specifically broken out under (b)(2). And then, lastly, we get to those surreptitious listening items. And this is probably a new term for a lot of people in this room, because we don't really think of these as being encryption products, for the most part. So, I'll give you an example of a typical surreptitious listening product. It's equipment for intercepting a telephone conversation, whether it's analog, cellular, or Voice over IP. Now, think about that for just a moment. There's all these parts of the telecommunications switch, and the technology required to actually intercept a phone call instead of simply routing the phone call is really no different. It's the same hardware -- it's just a slightly different installed piece of software in there that performs slightly differently. It's recording the telephone conversation as it passes by or routing the telephone conversation to someone for recording, instead of simply routing it to the intended destination. So, I've had a lot of conversations in the last year about companies who simply added this feature to their existing product and hadn't really thought about how adding this feature to their Voice over IP switch has now actually caused it to start recording the private content of telephone calls and what the consequences of that are. So, this is not to make you all worry all of a sudden that your telecommunications switches are all controlled with surreptitious listening devices, but to raise a little awareness that, if you start moving towards -- you know, if

you start installing features in that direction to be aware of these concerns ahead of time, so that you don't find yourself in the situation where we can't grant the license for the product to go out of the country. And the reason is we don't administer the Wiretap Act under Commerce. And possession of one of these items without authorization is a felony. So is sale. So is marketing. So is exporting it. So is development. It gets ugly pretty quickly. And the general structure is the Omnibus Crime Control and Safe Streets Act, but more specifically, the section that deals with this is commonly known as the Wiretap Act. And if you want to get more familiar with it, it's 18 U.S.C., sections 2510 through 2522. I'm assuming that the takeaway that most of you really want to know today, though, is that License Exception ENC does not authorize export of these items. For our purposes, it doesn't make any difference at all whether the item has encryption functionality or not, because there's still this law in place that controls how they're applied, and, you know, the export is just not the primary concern here. Licenses are required for export to all end users, all destinations, and there's a general policy of denial. The exceptions are for U.S. government agencies or communication-service providers there in the normal course of their business. So, if you're representing a U.S. law-enforcement agency and you're partnering with some other organization in another country and you need to send something out of the county, you know, contact us. Licenses are authorized for that situation. If you represent a telecommunications company and you receive court orders for wiretaps from the local law enforcement and you have to comply with those court orders, you know, that's one of the few circumstances in which we can grant a license. And you wouldn't think there would be that many licenses for these products in general in a year, but the rate at which they're coming in has just exploded over the course of the last 2, 3 years. I mean, I think I went from getting one a year to like five times as many, and then again, it's at least doubled or tripled in just the last year. Anyway, something I'd like you to understand is this structure that we have for authorizing these does not authorize sales to integrators for future sales. The end user has to be a party under contract, and it's got to be one of these situations that's specifically allowed under that Wiretap Act and under our regulations. And it also doesn't matter if the item was of foreign manufacture and was brought into the country. It can create problems when you import an item into the country for, like, a demonstration to a law-enforcement agency, and then you want to return it to the foreign manufacturer, because, unless it's

in compliance with this section of the policy, we can't authorize it for export to go back out again. So, I don't want to try to make you experts in surreptitious listening stuff today, but I would encourage you to contact us early in the process if you want to export items that now may be -- that may be SL-controlled. And the reason is we can try and figure out a way to do this in an intelligent way, where you aren't left with either products that you can't sell or products that you may or may not be in violation of the Wiretap Act for simply possessing. And I wish this was a hypothetical case, but the last year has shown me that it's anything but. Now, if we flip this over, there's a comparison chart. It's mostly gonna review what we just said a moment ago. And if there was one and only one line I'd like you to really understand from this chart, it's the technology for these different classes of products is really not that different. But License Exception ENC does not authorize export of any of the surreptitious listening items. They require licenses for every export and every destination. And if you've gotten used to the License Exception ENC and the authorization for, you know, sending National Security controlled items to Canada, for example, even Canada requires a license for these. There aren't any exceptions. All right. Now, there's new product descriptions under 740.17(b)(3) and 742.13(b) -- 742.15(b)(3), which is the Mass Market counterpart. What I'd like you to understand most importantly from this slide, I believe -- we'll start off with, anyways -- that nonstandard cryptography includes WAPI. If you manufacture a product with WAPI functionality, it's going here. If you manufacture a product that you think would be one, but it includes a WAPI chip, even if you're not using the functionality, then we're gonna have to drill down a little deeper to determine which of these three fact patterns applies. Now, the first fact pattern is when the WAPI functionality cannot be used -- it's just disabled or it's not powered or there's some physical impediment to it being used. And that's easy, because we don't even consider that to be, you know, active encryption technology at that point. And the second is that the WAPI functionality is dormant, but it can be used with some sort of cryptographic activation method. And at that point, we really do have to start digging a little deeper. The third fact pattern is that the WAPI functionality is sitting there, but it's just not used. So, in general, under that first fact set, we do not consider that product to use nonstandard cryptography because the WAPI functionality is disabled. In the second fact set, we consider the particulars of the activation method and we want to discuss that activation method with our

colleagues from the NSA to decide whether or not we consider it effective. In the third fact set, it's (b)(3). Even if you're not using the functionality, if it's just sitting there and there's no impediment to the user using it for whatever they want, then it's kind of like the laptop that's been, you know, shipped with a chip in it and you simply haven't provided the driver. So, if it's easy for the user of that product to install the software on it themselves, we can't just ignore the fact that that functionality is present. Now, classifying products that include nonstandard functionality, even if it's not used, requires a deeper level of understanding and inquiry. So, sometimes, it's problematic - someone comes in and they ask for a (b)(1) classification for the product, and we learn from their description that it's got a WAPI chip in it. And they say, "Well, we're simply not using that functionality." Nevertheless, we're gonna have to have a deeper conversation and understand, you know, which of these patterns applies. And I mention that because, when we don't have that information up front or -- you know, it delays the process, and it doesn't have to. If we can quickly figure out which of these three fact patterns applies, or, better yet, if you could discuss it in your letter of explanation, as to, you know, how we ought to be applying the fact patterns and what the situation is here, the thing moves through the process much more smoothly because, as Anita mentioned, the (b)(1) products we can classify ourselves -- we don't even have to send them out to NSA. So, we're talking turnaround time on your classification on the order of a week or two, instead of in excess of 30 days. This is an issue because a lot of manufacturers have network-infrastructure products -- you know, if a chip has WAPI in it, but it has like nine other functions that they want -- it's available on the market first, or it's cheapest, or, you know, they can get it now from an existing manufacturer and it's in stock, but they have to wait for another source, then they're gonna go for that product. And you know, this creates an issue where we have to dig in a little deeper. Anyway, I won't belabor the point, but I would encourage you to discuss that with us during the round table this afternoon if you believe your products might be in that category. Also, I'd like you to -- remind you that (b)(3) items cannot be self-classified, and this applies to all the other (b)(3) items on this chart, as well. And then, finally, (b)(3) also includes an item about cryptographic enabling keys. And we haven't forgotten about it, but Aaron's actually gonna cover that topic in greater depth as soon as he comes up and gives his presentation. So, with that... I see the time is almost 10:30. Would you like to speak again, Randy? It looks like you're getting up.

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

>> [Chuckles]

>> Randy Pratt: Thank you, Mike. I was just going to remind you that we're going to go ahead and break for coffee, and then we'll come back, and we'll address some of the questions and answers that we have received on the first set of presentations before we start our second set.