Transmission and Transportation Webinar
January 17, 2013

And thank you for standing by. All lines will be in a listen only mode for the duration of today's conference call. This call is being recorded. If you have any objections you may disconnect at this time. Now we'll turn the meeting over to Ms. Treva Alexander.

Good afternoon everyone like she said my name is Treva Alexander and I'll be your host for the next 30 minutes. I appreciate you taking the time out of your busy schedule this afternoon to receive this valuable nugget of information. Now folks who have taken courses with CDSE in the past, you know there are always administrative announcements, so let's take a moment and review those administrative announcements.

If you take a look at the screen and become familiar with the layout you'll find a question and answer box there and you can submit questions, however due to the large number of participants, we may not be able to answer all of the questions that are posed during the webinar, but don't fret, because in a few days we'll follow up with the webinar we'll have frequently asked questions posted on our website. You'll be able to find those where you see the description of the webinar posted. Also see that you can download the presentation slides, so if you click on the File Share box below, you can print the presentation and you can take notes as I actually discuss the slides. Enclosure 4 of the DoD Manual 5200.01 is also provided in the File Share box. And this reference material is the detailed policy guidelines that is related to all of the main points presented in today's webinar. You'll also see two Job Aids that are handy references and you can download those and print those. Now as I conduct the webinar, you'll notice that questions will appear on the screen. These are poll questions merely designed as a knowledge check. So if you could respond as quickly as possible and then what I'll do is I'll discuss the answer and then we'll move forward.

Let's go ahead and get started with a poll question. It says where can you find information regarding the proper wrapping of classified items for transportation? And I see most of you are responding as Volume 4. Actually the correct answer is Volume 3 and we're going to talk about that as we move forward. I want to thank everyone for responding so quickly. Now the DoDM 5200.01, Volume 3, Enclosure 4, actually specifies that components have to establish procedures for transmitting and transporting classified information that maximizes the accessibility of classified information to individuals who are eligible to access, and it has to minimize the risk of compromise while permitting the use of the most cost effective means. Now what does that really mean to us? That we're responsible for utilizing government funds in the most cost effective manner possible while still maintaining the integrity of our classified information. And for the most part anyone transmitting or transporting classified information is responsible for ensuring that the intended recipient is authorized access and that they have a need to know, and that they have the capability of storing that classified information in accordance with the

requirements we're going to talk about throughout this manual. So let's go ahead and take another poll question.

Holders of classified information can share content with agencies outside of the DoD. Now I know that we haven't yet discussed that, but I just want to do a knowledge check here real quick. So it looks like we're kind of half and half. The answer is true and we're going to talk extensively about that. Thank you again for responding so quickly.

Classified information that originates in another DoD component or department or agency other than the Department of Defense may disseminate to other DoD components or to other U.S. departments or agencies or to U.S. entities without the consent of the originating component, department or agency. Now there's some criteria that goes along with that. For access, the access is actually outlined in Section 3, Enclosure 2, of Volume 3. And as long as those requirements are met, then we can disseminate the information to another person. The classified information is not marked as requiring prior authorization for dissemination to another department or agency and we would see that marking as "ORCON." The other thing is the document had to have been created on or after June 27, 2010. Now this date is very key because it's the effective date of the 32 CFR Parts 2001 and 2003. Now our listeners may know that as the Information Security Oversight Office implementing directive to the Executive Order 13526. Now if the documents were created before June 27, 2010, then they cannot be disseminated outside of the Department of Defense without the originators' consent. Another note to that is documents created on or after June 27, 2010 whose classification is actually derived from documents created prior to that date, cannot be disseminated without the originators consent either. Now I know that's a lot to process, but you have your slides, and you're taking your notes so you can go back and reflect on that later. Let me mention one more thing about disseminating outside of the DoD. As you can see on your screen, according to Executive Order 13549, dissemination of classified information, state, local, tribal and private sector officials shall be in accordance with implementing guidance issued by the Department of Homeland Security. Now that classified information originating in or provided to, or by the Department of Defense may be disseminated to a foreign government or an international organization of governments, or any element thereof, as long as it's in accordance with Executive Order 13526 and the DoD Manual 5200.01. Now dissemination of information regarding intelligence sources, methods, or activities must be consistent with the directive issued by the Director of National Intelligence.

Now if you notice on your screen there's a caption of a job aid that CDSE has actually put together and it details transmission methods and requirements for the different classification levels such as Top Secret, Secret, or Confidential, and you can also find that in Volume 3, Enclosure 4 of the DoD Manual, so you can take that, you can actually download this job aid from the File Share box and keep that as a handy tool for you to reference. Now let's take a moment and review transmission methods via secure communications. So transmission of DoD information has to comply with COMSEC measures and procedures that are actually identified

in the DoDI 8523.01, and any computer to computer transmission in addition to meeting the requirements of the manual, has to meet, has to make sure that it's been accredited in accordance with Intelligence Community Directive 503. Now another important thing to note is that electronic transmission of classified information over secure communication such as secure email, is actually the preferred method versus physical transfer of our hard copy documents. Now we have to make sure that when we're transferring our information via electronic means or any other means, that it's properly marked. So be mindful of that, and you can check the markings if you need guidance on that in Volume 2 of the DoDM. Let's take another poll question very quickly. Are coversheets required when transmitting information over secure fax? Now once again I know we didn't cover that, but we're going to talk about that very shortly. And I see here that most of you answered correct, that is correct that you do need a cover sheet. Thank you for responding so quickly. Folks, I'd like to emphasize just this one thing. Only secure facsimile equipment can be used when we fax classified information and always, always be mindful that when you're transmitting information via fax, that the recipient has the appropriate clearance and the need to know. You also want to make sure that their secure communication is at the right level of classification. So if you're transmitting Secret information then that secure communication should be cleared at the level of Secret or Top Secret.

Now on your screen you'll see an example. It's just a sample of a fax cover sheet, we're not saying this is the one you must use, but it's a sample. Your component will give you guidelines on how to develop your fax cover sheet. Now we just want to emphasize the actual components that must be encompassed in the fax sheet. So you have the fax cover sheet there, and this is for transmitting our classified material. It has to be conspicuously marked with the highest security classification of the information that's being transmitted and any control markings that are associated. The cover sheet also has to include the originators' name, the organization, the phone number. It should have an unclassified title, the number of pages, and the receiver's name, the organization, and phone number. Now when the cover sheet contains no classified information, it has to indicate unclassified when classified attachments are removed, and you can see that there on the screen.

Now let me reiterate that documents transmitted via fax also have to have the markings required for a finished document. So we shouldn't be transmitting any working papers or things of that nature. And we have to make sure that it indicates any control markings, and safeguarding for that particular material. Let's talk a little bit about secured telephone conversations. Now only approved secure telephones including cell phones, and phones such as personal electronic devices authorized by the Director of NSA can be used for any of those classified conversations. And users have to ensure that the secure communication that the secure connection is at the appropriate level as the classification of the conversation.

Let's look at how we want to package our material when we're going to mail it off. So first we need to ensure that our classified information is enclosed in two opaque sealed envelopes, wrappings, or containers. They have to be durable enough to protect the material from any

accidental exposure, and we have to be able to tell if someone actually tried to tamper with our material. So how we do it is we prepare a package and securely seal the material in ways that minimize the risk of accidental exposure. And we do that by making sure that it's not in direct contact with the envelope, so when we put our classified material inside the envelope on your screen you have a classified cover sheet and envelope and you have some tape. What we would do is take either a cover sheet and place it over our classified material before we put it inside the envelope just to make sure it's not in direct contact with the envelope, or you could take the material and you can fold it so that it faces each other and that way it's not in direct contact with the envelope. Now CDSE has actually put together a handy dandy video and this video will give you guidelines on how to package the material in a secure manner, and you can access that at the end of this webinar—we'll have a link directly for you. Let's talk a little bit about the outer envelope. So when we address the outer envelope it should contain an address to an official U.S. Government activity, or to a DoD contractor with a facility clearance and that we have to make sure that they have the appropriate storage capability for our material before we're mailing it to them. The other thing that we want to do is we want to make sure that we use a complete return address well sender address. So you don't just have the sender's name. It has to be the complete address in the top left hand corner. Now when we package our outer envelope, I'm sorry, our inner envelope, we have to make sure that we send the, that we have the complete senders address on there as well, and that we have the address of the activity that we're sending it to. Now this is where we can put address to a particular person, or an attention line, and we also have to make sure that we put the highest classification level of the material on this inner envelope. And any restrictions such as Restrictive Data, or NATO, and any other control markings that need to be noted on this inner envelope as well. Now what we don't want to do is we don't want to put any classification markings at all on the outside of the outer envelope. And we want to make sure that we don't put any other unusual markings on the outer envelope that's going to draw attention to our classified material. However, we can put "Postmaster: Do Not Forward."

Now if the classified material is an accessible internal component of an item of equipment, the outside shell or body may be considered as the inner enclosure provided that it doesn't reveal any classified information, just as you see the picture on the screen. Now if the classified material is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered a sufficient enclosure provided observation of it doesn't reveal classified information. Just as you see on the picture on the screen. Now if the classified material is an item of equipment that cannot be packaged, or the shell or body is classified, it shall not be, it has to be concealed with an opaque covering hiding all the classified features, such as the pictures you see there on the screen. Let's take a quick poll question.

When using a briefcase for classified transports, where should the key be kept? And I see some folks, I know we didn't talk about it but, so it looks like most of you indicated the correct answer. It should be placed in a separate sealed envelope. And let's talk a little bit about that.

Thank you for responding so quickly. Now for the remainder of the webinar, we're basically going to talk a lot about hand carrying of our information. A locked briefcase or zippered pouch made of canvas or other heavy duty material is usually what's utilized when folks are transmitting classified material from one activity to the next. Now when you are using those briefcases or zippered pouches, it has to have some type of locking mechanism that's integral, and we take that key like we said before and that's placed in a separate envelope. Now these types of cases are also used to restrict access of our classified material, say if you're taking it to another activity and the recipient is not actually there, then you're going to lock that pouch, take that key and have them stored separately, that pouch has to actually be locked up if the recipient is not available for receiving that information and it should be locked in an approved GSA container. Now if you see on your screen there's a picture of a tag because the briefcases or the zippered pouches that you're utilizing have to have some identification on it, it needs to display the name and the street address of the organization that's sending the classified material. It should also have the name and the telephone number of the point of contact of the sending activity on the outside of the briefcase or the pouch or on some type of tag just as you see there on the screen.

Now as indicated on the slide, you have to serialize your pouch or your briefcases. Now this is and it should be done on the exterior of it so that it's readily available and someone can see it. This is mainly for tracking purposes. When we have a locked briefcase or a pouch that we're utilizing, the activity that's utilizing it has to be able to keep track of that and make sure that they have it and can know exactly where it was delivered and when it was delivered and to whom it was delivered to. And as I said earlier, if we leave that material and the recipient is not there to receive it, it has to be locked up in an approved GSA container at the highest level of classification for that material encompassed.

Last note: Ensure that the activity authorizing the use of the briefcase or the pouch, like I said maintains an accounting system for that briefcase. Remember Heads of DoD components are responsible for establishing procedures to ensure that the hand carrying of our classified material is minimized to the greatest extent possible and that it doesn't pose unacceptable risks to our information. Hand carrying is permitted in locations when other means of transmission is not used, so remember we said earlier that secure communications is the preferred method for transmitting our information. So at all costs try and utilize that method before you're actually hand carrying or couriering the information. Now let's talk about hand carrying, who's actually authorized to hand carry and why. Information should be hand carried only when it's not available at the destination and that it's operationally necessary or contractually required. Another reason why we want to hand carry our information is because it can't be sent via the secure email or fax. We want to make sure that the appropriate officials authorizes the hand carry according to the procedures established at the DoD component, so like I said before, Heads of DoD components have to establish those procedures. At times hand carrying is accomplished aboard a U.S. carrier or a foreign carrier if no U.S. carrier is available and the U.S. escort retains

the custody and physical control of that information. Now anytime we're hand carrying, arrangements have to be made for secure storage of our classified information at a U.S. Government or a cleared contractor facility.

Now individuals hand carrying or serving as couriers or escorts for classified information, must be informed of and acknowledge their security responsibilities as it relates to hand carrying that classified material. Now this is a great responsibility and we're going to talk about it because they have a lot of responsibility. The individual has to understand that their liable and responsible for that material that their carrying. The material is not under any circumstances to be left unattended. Now if they have to stay overnight somewhere, then arrangements have to made for storage of that classified material in a U.S. military facility, an embassy, or a cleared contractor facility. And under no circumstances can the classified material be stored in a hotel safe. I don't know of any GSA approved safe that are in hotels, I'm not saying they're not, I just don't know of any, so for now don't ever store classified material in a hotel safe. The materials cannot be opened in route except for specific circumstances and we're going to talk about that next. And the material should never be discussed in public, in any public place. You're not supposed to deviate from the authorized travel schedule, and in the case of an emergency the individual must take measures to make sure that they're protecting that classified material. The other thing that they have to make sure of is that all of their travel documents are current, complete and that they're valid, such as a passport or courier authorization and any type of medical documents that they might have, those have to be current.

Now as I said earlier, it is a lot of responsibility. Now arrangements must be made in advance with customs police and or immigration officials to facilitate the movement through security. Now we talked earlier about there might be some instances where that material might have to be opened, okay? Now just because we made arrangements ahead of time, it doesn't mean that we're assured from immunity and that the information won't be searched. But what we should do is when we're approaching that secure area, we should ask to speak with the officials that are in charge and show them our travel documents so that they know that we're traveling with some material that needs to be protected. A lot of times that may suffice, and get you passed through unopened, but it's not a guarantee. So if the senior official actually demands to see the contents inside the package, the first thing that we should do is take that security official and ourselves and the material to a private area where we're not exposed to the public, and then our role as a courier is to ensure that we're only opening and exposing the security official to as much of the information to satisfy them for their inspection. Now what we should do after that is make sure that we have them help us repackage that material so that when it's closed up and sealed, they should be signing across the seal and then we want to have them notate on our travel documents that they opened it, that it was opened due to an inspection.

Now classified material to be carried by a courier must be inventoried and a copy of that inventory is actually retained at the originating area where it came from, and then the courier, as couriers we should have a copy of the information versus the original of it. Now upon return, the

courier must return all the classified material in the sealed package and produce a receipt signed by the security officer from the organization where it was delivered to. Let's take a poll question real quick. DD Form 2501, which is the Courier Authorization Card, is valid for how many years? Looks like, okay, so with the new launch of the DoD Manual, it specifically states that the courier card is valid for 2 years, so thank you all for responding so quickly. Let's talk a little bit about that.

So typically when that courier card is issued, it's only issued because a person has a reoccurring need for transmitting or couriering classified information, it's not because they're hand carrying it one time. The courier card itself is issued and signed by an official at that actual component, because these are controlled items, the DD Form 2501, so you just can't download it from the internet. As we mentioned in the poll question, it is good for 2 years, it should be issued for no longer than that, and then when it comes up on reevaluation after that 2 years, a new courier card should be issued with a new expiration date. So you should never see a courier card that says indefinite in the expiration date section. The use of the DD Form 2501 for verification of authorization of hand carry for SCI and SAP, there should be some specific procedures already in place at your component as it relates to those special programs.

Now remember a few slides back I actually mentioned briefly about receipts. Receipts are required for all transfers of classified information and material to a foreign government. Now there's the receipts actually served two important purposes here: First, they document the transfer of the security jurisdiction between the two governments, and then the other purpose is to alert the recipient government that the information and the material has been transferred. So that lets them know now you're responsible for protecting this information or material in accordance to the agreements and arrangements that are in place. Now most foreign governments actually waive the receipt requirement for their restricted information.

Transmission of classified information to a foreign government by IT and communications systems has to, at a minimum, be audited to assure that the intended recipient sees that information. Now folks, I know we covered a lot of material over this time period and I just want to make sure that I reiterate to you, I talked earlier that CDSE has a video that's in place that you can watch and it's going to give you step by step guidelines on how to package our classified material before we're actually mailing it. So that link is there for you, you can actually click on it on the screen and it will hyperlink you right to the CDSE website. We also have some other handouts as it relates to Transmission and Transportation, and those are located on the CDSE website. Again, there's a hyperlink there on the screen. And if you have any additional questions regarding any security related questions, we have a mailbox there for you. You can click on that and myself and the other folks here, we are available and can answer the questions for you.

Folks I want to thank you for tuning in and I appreciate you responding so quickly to all the poll questions that were addressed. And that is our time.