Storage of Classified Information Webinar November 15, 2012

Welcome and thank you for standing by. At this time all participants are placed on listen only mode throughout today's conference. Today's conference is being recorded. If you have any objections, you may disconnect at this time. Now I would like to introduce Treva Alexander, you may begin.

Good afternoon everyone, welcome to the CDSE webinar—and like she said, I am Treva Alexander and I'll be your host for the next thirty minutes. I appreciate you taking the time out of your busy schedule this afternoon to tune in. Just before we get started I'd like to cover some administrative announcements, so if you take a look at your screen and get familiar with some of the layout there—you'll find a Q&A box and that's just over to the right of the screen where you can submit questions throughout the webinar and then we'll address those questions. Now, because of the short time and the number of the participants we may or may not be able to answer all of the questions posed, but, you can look at those questions later on once we post it on our frequently asked questions on our website, on the CDSE website.

Alright, so you also see that you can download the presentation slides and we also have an enclosure, Enclosure 3, that you want to go ahead and download and follow along with us because all of the information that we'll be referencing this afternoon comes from the DoD Manual 5200.01, Volume 3, Enclosure 3, and we have put Enclosure 3 for you to follow along throughout the webinar. You can also take notes if you go ahead and print out or download your presentation; we have it so that you have "Notes Section" over there on your screen and if you print it out. So to answer any other questions that you may submit we'll go ahead and review those throughout the webinar as well. As I conduct the webinar you might see some poll questions, those poll questions are merely there for like a Knowledge Check, and as you see the question on the screen if you could go ahead and respond to the question as quickly as possible and then I'll go ahead and discuss some of those answers. You also have the option of viewing in a full screen if you want to do that, your screen can go in and out of full screen, however, when you 're in the full screen mode you have to go back in to the area where you can answer your poll question in the Question and Answer section.

Rachel is one of our producers here and she's going to be the person that's going to post our poll questions on the screen for us, and so we're going to get started with a poll question. Rachel, if you could bring that poll question over for us. Okay, and so the question that we have here is "Which form or forms is or aren't a security container check sheet?" If I could get everyone to go ahead and respond—and it looks like most of you are very familiar with the forms—and that's an indication that you're familiar with their uses, which is really good because we're actually only going to go into detail about one of the Standard Forms, which would be the SF

700. The answer is actually the SF 702—that would be C—and I want to thank each of you for responding so quickly. Now as I said earlier all of the information that we're going to talk about comes from the DoD Manual, it specifically indicates that classified information shall be secured under conditions that are adequate to deter and detect access by unauthorized persons which represents acceptable security standards. Now, you may ask what are those acceptable security standards—well, some of those acceptable security practices would be not to store items such as weapons, funds, jewels, precious metals, or drugs in the same container that we store and safeguard our classified information. And also one of the things we want to be mindful is to make sure that all of our classified holdings that we're keeping on hand are merely those that we need for our mission and that we're reducing them as much as possible. And the way we do that is we have our annual cleanout days and I'm pretty sure that all of our listeners out there are actually exercising their annual cleanout days as we're required to do. The General Service Administration establishes and publishes minimum standards, specifications, and supply schedules for our containers, our vault doors, our modular vaults, our alarm systems, and all of those associated security devices we find suitable for storing and protecting our classified information, while the Director of National Intelligence actually establishes the security requirements for those sensitive compartmented information facilities. And when we remove our classified information from our storage containers we're required to make sure that we keep our classified material under constant surveillance, and one of the ways that we do that is we utilize our cover sheet—and as you see there on the screen, we have a display of the SF 703, which is the Top Secret cover sheet, the SF 704, which is the Secret cover sheet, and the SF 705, which is the Confidential cover sheet. Now just by their mere color and some of the identification on the cover sheet you can tell that which cover sheet goes with what type of information. Another good practice to use the cover sheet for is to prevent inadvertent disclosure of our classified material from anyone that is just walking by casually.

Now, some of the other things that we want to make sure we're exercising is our end of the day checks. Our end of the day security checks are there in place to ensure that we have a system in place so that at the close of every business day we secured our classified material appropriately. Now the SF 701 that you see there before you on the screen, that's the activity security checklist and that's how we record that we secured our material at the end of the day. Now using your chat option, if you could tell me some of the things that we typically see on our SF 701. *(Pause.)* I see some of you are responding check the printer, time opened, check the printer, time closed, safe closed, okay, so CAC removal—yes, definitely, doors and windows are secured—yes, absolutely—and those are some of the things we do see on our SF 701, and folks what I want to encourage you to do is to ensure that we're placing those items on our SF 701 that's actually pertinent to securing our classified material. You know sometimes people put on there "shut off the coffee pot or turn off the light"—you know— is that really pertinent to the classified material to shut off the lights? But just be mindful of that. Thank you so much for your quick responses.

The SF 702 is also an integral part of our security checks and what we utilize the SF 702 for is to make sure that we're logging the opening and the closing of our security containers, as well the person is initialing stating that they did either open or close the actual containers. So we want to make sure that when we're utilizing our 702s and 701s that we pay close attention to our Component's records management schedules just to know how long we should be maintaining those forms on hand. Now remember I said we're going to go into great detail about the SF 700. This is our form here—and this is a really good form to use—and not only that, it is required and we actually have some new requirements that were integrated with the new DoDM and I want to talk to you about those. Now when the information on this form is completed, the record should be maintained for every container or vault or secure room door used for storing our classified information. Now every time that we actually change the combination on our container we have to record this on an SF 700, so we have to make sure that we're doing that. I'm sure that we all understand the SF 700 is a two part form, so let's go ahead and look at Part 1.

Part 1 of the SF 700, when it's completed, it's unclassified, however, there is personal identifiable information on there—and what I mean by that is you record the person's name, address, and telephone number who would actually be called in the event that container is found unsecure. So if you notice there on the first picture you have the Part 1 of the SF 700 and it's placed in an opaque envelope. That opaque envelope should be sealed—and on the outside of it if you notice in the center picture you need to write on there "Security Container Information." That alerts the person who finds the drawer or the container unsecured that that's what you need to pull out and open up to start calling the persons on that list of that SF 700 form. So if this happens, say the seal needs to be broken and it's after working hours of course, and there's not another opaque envelope available, then you can utilize the same envelope to reseal the SF 700 as best as possible, but when you get to the next working day you must obtain a new opaque envelope and reseal that SF 700 in there, again, that's personal identifiable information that needs to be protected. *(Pause.)*

And then Part 2 of the SF 700, when it's completed, it is considered classified, and so it's classified as the highest level of classification authorized for the storage container. And it must be sealed and stored in accordance with the SF 700 instructions so you know that once you record your combination on Part 1, I'm sorry, on Part 2 which is that first picture you see there, with the combination recorded, you're going to flip it over on the back, which is the middle picture that you see there and you're going to complete your classification authority block. Yes—you have a classification authority block that you have to complete. So you want to put classified by, that would be the custodian who's completing the actual form, then you're going to put "Derived From: 32 CFR 2001.80(d) (3)," and then you're going to put declassified on, upon change of combination. Now you're probably wondering where did we retrieve the derived from information. That's actually pulled from the Information Security Oversight Office Classified National Security Information Final Rule to the Executive Order 13526. Make sure that we are

actually paying attention when we're completing Parts 1 and Parts 2 of our SF 700, it's very important.

Let's take a look at working from home. Now I know that's a touchy subject, and some people believe you can't actually take classified material home to work on, well—that's not true. When it's mission critical—and just let me reemphasize that—it must be mission critical for individuals to remove classified information and materials such as IT equipment and any associated storage material for working at home then specific measures and approvals are required. Now some of those security measures and approvals for the level of classification must be in place to provide adequate protection and security-in-depth, and to prevent access by unauthorized persons. So let's look at some of those requirements. So for Top Secret information, only the Secretary of Defense, the secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, Combatant Commanders, and the appointed senior agency officials can actually authorize removal of Top Secret information from the designated working area to take home. Those same officials can also authorize the removal of information for work at home for the lower levels, like Secret or Confidential. Now, DoD Component Heads can authorize removal of Secret and Confidential information from designated working areas to work at home; however, their authority cannot be delegated below the major command or equivalent level. So there are some additional requirements that go along with that. They also have to ensure that there is a GSA-approved security container that's furnished with a residential storage of the information, there has to be written procedures in place to make sure that there is protection available for the classified material that we're taking home. And there also has to be a record of what material was taken home. There is an opportunity to take classified material home, but again, these procedures must be in place. In the event that classified IT systems or equipment is going to be used with the working of the material at home, you might want to take a real close look at Volume 3, Enclosure 7, Section 7, and you also want to pay strict attention to the DoD Instruction 8510.01—that is the DoD Information Assurance Certification and Accreditation Process, and those are important to review. Now this is the last thing we're going to focus on for work at home, and that's in the event you're in a foreign area and you need to take the work home. Work home may be authorized in foreign countries only when the residence is in a specific location where the United States actually enjoys extraterritorial status, such as an embassy, a chancery, a consulate compound, or a U.S. military installation.

Alright so we've talked for a little bit, let's go ahead and take another poll question. Rachel is quick and swift, and got our poll question up already. Alright, so who establishes and publishes uniform standards, specifications, qualified product lists or databases, and supply schedules for security equipment designated to provide secure storage for our classified information? And it looks like most of you were listening, oh my goodness! Okay, that's right—B is the answer, GSA. Thank you all so much for responding so quickly.

So now for the sake of time we won't actually go into great detail about our lock specifications but very briefly except as provided elsewhere in the DoDM, the combination locks on our vault

doors, our secure rooms, and our security containers protecting our classified information must conform with Federal Specification FF-L-2740. So what you want to do is get more familiar with that guideline, and guess what—CDSE has some great resources to help you out with that! We have some security shorts, one in particular is our "DoD Locks Approved to Safeguard Classified and Sensitive Material;" we also have some training videos that are very helpful so if you need some help walking you through changing a combination or operating the Sargent and Greenleaf 2740 locks, you might want to reference those training videos, as well we have those same training videos available "Changing a Combination and Operating our XL 7 and XL 9 Locks," so take a look at those from our CDSE website—you will be very impressed I promise you.

Now let's take a look at classification levels by storage. So for Top Secret information, we have the option of utilizing a GSA-approved security container, as long as we've employed one of the following supplementary controls. So either we have an employee who's cleared at at least the Secret level for inspecting the security container once every two hours, or the location that houses our security container is protected by an IDS system and it meets the requirements of Appendix 3 of the DoDM, and that we also have personnel responding to the alarm's annunciation within 15 minutes. The other option would be of course we employ the GSA security container is equipped with our lock meeting the FF-L-2740 specifications, of course as long as the container and the area surrounding is security-in-depth. The other option is we could store our TS material in an open storage area, which is also known as a secure room, as long as it's constructed according to the requirements indicated in Appendix 3 as well, and that it's equipped with an IDS system. There has to be personnel readily available to respond to the alarm's annunciation within 15 minutes. And that's as long as it's been determined that the area has security-in-depth. Now in the event it does not have security-in-depth, someone must respond to the alarm's annunciation within five minutes. We also have the option of storing our Top Secret material in a vault, or a GSA-approved modular vault, as long as they meet the specified requirements of Appendix 3. Lastly, under field conditions because there are those that exist, military commanders actually have the authority to make the judgment for the use of the storage device or the security control measures adequate to prevent unauthorized access of our Top Secret information. However, before they actually make that decision, they have to make sure that they've exercised risk management methodologies to determine the appropriate safeguards. And we're going to talk a lot more about those risk management methodologies a little bit later in the webinar.

Now when we talk about Secret of course we can employ any of the methods available for Top Secret for the protection of our Secret material. We also have the option of storing our Secret material in a GSA-approved container or a vault built to the specifications indicated in Appendix 3 without those supplementary controls. Now we can also place our Secret information in an open storage area meeting the requirements we stated earlier as in Appendix 3, provided that the senior agency official determines in writing that security-in-depth exists and one of the

supplemental controls are utilized. Now either there is an employee cleared to at least a Secret level inspecting the open storage area once every four hours, and notice that's slightly different then Top Secret, because it was every two hours for Top Secret. Or there's an IDS system meeting the requirements in Appendix 3, and that there's someone responding to the alarm's annunciation within 30 minutes—and notice that's slightly different from Top Secret, because for Top Secret it was every 15 minutes. We also have the option of storing our Secret material in a secure room that has been approved for storage for Secret information by the DoD Component prior to 1 October of 1995 as long as the DoD Component reassesses the requirements for the secure room and makes plans to bring that room up to standards according to the DoDM by at least 1 October of 2013. And that's again as long as security-in-depth exists.

Now as far as Confidential information, we know that Confidential we can utilize any of the methods for Top Secret or Secret in order to protect our Confidential information. What I want to bring to your attention is we have a CDSE security short for classified storage requirements—there's an option for you to download the actual job aid and it will give you a breakdown with a matrix of storing your classified material at the different levels and how you can store them.

Remember I said we were going to talk about those risk management methodologies, notice before you that there's the five-step process for risk management. The very first thing that we're going to do is we're going to assess our assets, and when we do that we make sure that we identify our assets as our people, our information, our equipment, our facilities, our activities, and our operations, and what we do is we consider the storage alternatives specified for storage of classified information by the classification level that we just reviewed. And then we take our risk assessment to facilitate how we're going to put our security-in-depth in place. This will also help us identify and choose the appropriate supplemental controls that may need to be implemented and then our analysis should at a minimum consider all the local threats, both known and anticipated, and the vulnerabilities. Our assessment should also consider the existing security environment and controls, the ease of access to our containers, and other areas where our classified data is stored. And then we want to make sure that our assessment considers the criticality, the sensitivity, and the value of our information that's stored. And then the last thing that we want to do is we want to incorporate an analysis of the cost versus benefit of our potential countermeasures, and then what we'll do is we'll take our risk assessment and make a determination whether we're going to install an IDS, or whether we're going to implement any other supplemental controls.

Now real quick—procuring new storage equipment, for new storage equipment when it's procured, it's procured from the items list on the GSA Federal Supply schedule and we talked about that earlier. Now real quickly, when GSA-approved security containers or vault doors with locks meeting the FF-L-2740 are placed in service and when existing mechanical locks are replaced and they're meeting the specifications, we as the security custodian or the security manager have to make sure that we've recorded that information on our SF 700 form and that would be the serial number for our locks and containers that we have there. So if you need more

information with regard to procuring new equipment you want to reference the DoD Lock Program technical support hotline, that number is there on the screen for you or you can also visit their website for more information.

So looking there on the screen you have two security containers, Container 1 and Container 2. If you take a moment using your chat box and tell me which container is properly marked, Container 1 or Container 2? *(Pause.)* Now I see some variations in the responses, okay, so there are some myths out there that we need to actually dispel. So Container 2 is actually the one that's properly marked. Here's the deal folks, no external markings should be on the container revealing the level of classification of the information stored in the container or authorized to be stored in the container. No external markings. Now that doesn't mean that you can't place a mark or a symbol like a barcode, you know, just in case you want to use it for identification or inventory purposes, but you cannot mark that container stating the priority for emergency evacuation or destruction, you can't do that. And at times if you're a Component who's authorized to store intelligence information, the DNI might require you to put a decal or label on your container, and that's okay. But anything else other than what I just mentioned, no, you cannot place that on those containers—it's not authorized. Now in the event your GSA container or vault door has to go through a recertification process, you're going to have to remove any labels or barcodes that you actually have on that container, but after the container has been recertified, you can reapply those markings that you're allowed to put on there.

Alright, so entrances to our opened storage areas for classified information, let's go ahead and review that real quick. Now when areas storing classified information are occupied by authorized individuals, the entrances have to either be under visual control at all times to make sure that no unauthorized persons are coming in, or the entrance has to be equipped with an automated entry control system to limit the access. Now, some Components have a lot of money, and so you can employ some really elaborate control mechanisms: fingerprinting, hand geometry, iris scans, video recording, I'm sorry— video recognition—and facial recognition. Now if you're not a Component that has a whole lot of money, then make sure that you're utilizing your risk management methodology and you find those methods that are appropriate for the protection of your information at your component. Also the appendix to the volume here that we're talking about will give you more information on the standards for those access control devices, just understand that electronically actuated locks—like those magnetic strip card locks, those do not by themselves meet the required standards for protecting our classified information— and they cannot be used as a substitute for the locks prescribed that we talked about earlier.

Now for our foreign government information—I know a lot of people have questions about that, and that we've even had questions come into us about that, so—just so that we understand we're not trying to get people to actually purchase new containers or anything like that or spend a whole lot of money, so to the extent practical, your foreign government information should be stored separately from your other information just to facilitate control. Now what do we mean

by that? Okay, so to avoid costs you want to separate the storage just by placing it in a different drawer. You can still use the same container, just a different drawer, and of course if it's a really small amount of foreign government information, you can separate that just by file folders. You can have a file folder with your foreign government information placed in the same drawer with your other information. So just be mindful of practices like that.

Alright folks, that's the end of the webinar. I didn't go through it too fast and I want to make sure that everyone had the opportunity to hear some of the basic information. What I want to do is thank you so much for tuning in, what we will do is address all of those questions that we've had throughout the webinar and we're going to place those on our website— if you see there that our resources that we have available on our website is the www.dss.mil. If you go out there to our website you can see the webinar that's there and we will post the Frequently Asked Questions that were posed during this webinar and the answers to those questions as well. Once again, thank you folks for tuning in and I look forward to you tuning in for future webinars.