Security Education and Training Requirements

February 21, 2013 Webinar

Thank you for standing by. All lines will be on listen only for the duration of today's conference call. This call is being recorded, and at this time I'll turn the call over to Lisa Rainey. You may begin.

Thank you. Good afternoon everyone. My name is Lisa Rainey, and I will be your host for the next 30 minutes. I really appreciate everyone taking time out of their busy schedule this afternoon to receive another valuable piece of information as we progress through this Information Security series. But as usual, before we get into the meat of any of the information, we do have a few administrative announcements that we like to cover, primarily for those folks that are new to our webinar process. So if I could have you go ahead and take a look at the screen as we progress through this layout, you'll see that at the center right, at the top of your screen it says Q&A that is your Q&A box. That box is for you to be able to ask questions, you can type information or questions in the bottom, and they will populate in the screen. We will gather all of these questions, because due to the large number of participants today, we won't be able to answer all of those questions, but not to worry we will answer those questions, the questions will be posted to our frequently asked questions, or FAQ, on our website. And it will be in the same location where the description for this webinar is actually posted. Also if you look to the bottom left, you'll see a little box that says "file share", from the file share box you can print the presentations and take notes as I go through and discuss the slides. And as a bonus, we've also included Enclosure 5 of the DoD Manual 5200.01, and that's for you to be able to reference for any additional detail policy guidance related to some of the main points that we're going to talk about and present today. So as we go through the webinar you'll notice that questions will randomly appear on the screen, and these are what we like to call poll questions. These poll questions are just little knowledge checks that help us to kind of transition from one topic to another. If I would ask that you please go ahead and respond to those questions as soon as they're presented, and we'll discuss the responses after a number of you have actually entered your responses.

So having said that I do like start with one poll question, just to kind of get you in the flow of how they proceed. So this question asks: Where can you find information regarding security education and training? Now if you go ahead and put your responses in there, I'll see how much knowledge that you all have about where information is located in the DoD Manual. Looks like most of you are pretty much on point. You've got some pretty good responses in here. So the correct answer is DoD Manual 5200.01, Volume 3. That is the correct volume. That volume itself specifically talks about safeguarding our classified information, as well as our security

education and training requirements, so just remember that is the place you need to go to find more about security education.

So let's go ahead and get started. Primarily the Volume 3, Enclosure 5 of the Manual specifically gives you information that pertains to security education and training, and it does state that the heads of those DoD components ensure that their personnel not only receive security education and training, but that that training provides the necessary knowledge and information that enable quality performance of security functions. And it also has to promote an understanding of the DoD information security program, the policies that are contained within the requirements that have to be adhered to, and how they relate to national security and why they're important to our national security. In addition, your education and training should instill and maintain a continued awareness of those security requirements. And also assist in promoting a degree of motivation, and we always like to say a high degree of motivation, because as we know when folks are motivated, there's less chance of complacency. So just think about the times that you've actually been motivated, that you're more apt to go and do the things that are required of you. So if you take a look at the slide that's up now, what you're seeing is a poster from the security education. We do have posters on our CDSE website that are available for you to be able to download, and this can be part of your security education and training program. The regulation doesn't stipulate that you have to have one form of training, you can get training within your own component within your agency, you can use us CDSE, or even a combination of the two. But to go a step further you can also take the requirements from say Volume 3 and Volume 4 of the Manual, you can incorporate it into one overall training program. So you can kind of manipulate your training as you see fit and however it fits your organization, but as long as you're using multiple training mechanisms and techniques to get the points across that it requires.

So we're going to start off with talking about initial orientation this afternoon, and initial orientation really is going to set the foundation for individuals as they come into the information security program, and the manual does require that all personnel in the organization whether you're a DoD civilian, military member and even those on-site support contractors have to receive an initial orientation to the information security program. The orientation really covers a majority of all of what you need to know as it pertains to protecting our national security information. And if you look at the screen some of the topics that have to be covered in your initial orientation is the definition of what classified information is and controlled unclassified information, or CUI, and explain the importance of why that information has to be protected. Also it will give you a basic understanding of the different security policies out there that kind of coincide with our DoD policy, for some of you that might be in industry, well you have industry policy as well. And they kind of mimic one another to some respect, but you need to know what the policy says. Also notifying individuals of their responsibilities within the program, as it pertains to administrative civil and criminal sanctions that can be applied when appropriate, and when they say, "when appropriate" they're talking about in case of a security violation or

security infraction or unauthorized disclosure, then you'll be subject to those particular sanctions. It also provides enough information to make sure that you have the tools to be able to properly protect your classified information as well as your CUI, or controlled unclassified. And what are your responsibilities and what actions can you take if you discover information that is unsecure classified information that's not in a secure environment, or any other security vulnerabilities. One important piece is letting folks know that all information, the need to review all unclassified DoD information prior to its release to the public. As you know just because information is declassified, it does not mean that that information can be released. So all information has to undergo a review for release to the public.

So how many of you actually know who your security manager is? And I know initially when I was in security I had no idea who my security manager was and it's really important that you know that. Too often the people that we work with have no idea what the proper chain of command is for their organization, or even who they should report incidents to. So as part of the initial orientation training, if you are a security educator, you need to really consider putting in there who your DoD component senior agency officials are, and your activity security manager, who those personnel consist of, as well as a description of their responsibilities. Also the extent of their involvement in the protection of classified information, or controlled unclassified information, because if something happens you really need to know who do I go to and that should be covered in your initial orientation.

This slide really talks about initial access training. Outside of initial orientation, if you have access to classified information, and this is what we're going to talk about, this is when you finally receive your access to classified. Policy does state that all personnel receive training again on those policies and principles, but more specifically now how it pertains to derivative classification practices, because if you have access to classified information and you're not an original classification authority, or OCA, then you are a derivative classifier and you need to know how to process and handle that information, specifically the different levels of classified information and the damage criteria that's associated with them. Also they're certain restrictions on different kinds of information say Special Access programs, or SCI type information, or even NATO, certain restrictions on access, so you need to be familiar with them. And one other important piece of this is how do you respond if your question per say from the media about classified information. or to validate a piece of classified information, the existence of it. So there certain responses that are appropriate, so going to the regulation or even covering this information in your training is a necessity. So let's go with poll question number 2.

And that asks: What are some ways that you can fulfill the training requirements of the Manual 5200.01? And I see some of you are responding, we've got CDSE, I'm surprised everybody didn't pick us, but they're not but that's a good thing, we've got security workshop so you got component security manager, and the majority of you did pick all of the above, and you are absolutely correct. There is no one stop shop; training can be conducted by all of the individuals listed above. Very good and thank you so much for responding.

So, I want to talk a little bit about safeguarding and training. As we know that is one of our main responsibilities is being able to safeguard information, but more importantly understand why safeguarding is actually required. Within your agency if you have classified information we need to have processes and procedures in place because we generally use that information on a regular basis, we have to store it so we need to know the proper storage mechanisms that are authorized. Some information can be reproduced, some classified information has reproduction restrictions on it, so you need to know the rules for that as well. Transmitting information, well, there's only one venue that we cannot transmit classified information on and that's the unsecure side, so you need to know what those rules are. Also when we transmit information, well we mail it, we send it over secure websites, we hand carry it, so you need to know the many ways of how we can transmit as well as disseminating information and disseminating that goes to say that we do share information with other agencies. And destroying classified information, do you know if you can, or have the authority to destroy classified information, you need to be familiar with that.

One area of importance is emergency evacuation. In case of emergency you have to have processes in place to be able to safeguard or keep your classified information safeguarded, so you need to practice those mechanisms, you need to have policies in place to be able to identify how you're going to handle that if you happen to come into one of those situations. And how do you handle classified information, or where do you go, or who do you tell if information is not being properly protected. Don't think that you're doing something wrong if you tell on someone, but that is your responsibility, everyone has the responsibility to safeguard classified information. So poll question number 3, we're going to transition a little bit now really ask, who can identify the purpose of a security classification guide? And I know some of you think its bedtime reading if you've ever had one. Security classification guides are there to provide confusion, some of us might be totally clueless, but I would ultimately say that security classification guide are there to provide clear and concise guidance, and I'm proud to say that all of you have chosen the correct answer. And again thank you so much for responding. So to identify the main purpose of a security classification guide, yes it is a precise; a very comprehensive guide regarding specific programs, systems operations, or even weapon system elements. It tells you all the elements that are classified within a program, it includes those classification levels, and it also lets you know the reasons behind why a piece of information is qualified as being classified. And most importantly, it is how long you're going to keep that information classified, which is the duration of classification. When we talk about other special guidance, we're really talking about elements of compilation in your security classification guide. There should be special notes in there, if there's any other special requirements, if there's any dissemination restrictions they should be identified in that guide. And if you have elements of information that may or may not be classified, that when put together would warrant a higher level of classification, then those things should also be listed very conspicuously in your security classification guide. If you have a guide, those guides also have special requirements in that they must be approved and signed by the OCA that has oversight over that specific program, or

project. Your security classification guide has to be used as your main authoritative source for derivative classification. You should know that we have security classification guides, we have properly marked source documents, we have DD Form 254s, but to go to for derivative classification is your security classification guide, because that guide really ensures that like types of information are consistently given the same classification so it really qualifies consistent application for classified for classification. So if you've never seen one, if you've never heard of or actively examined a security classification guide, don't worry cause you are in luck because I'm going to give you several avenues on how to find classification guides, and where to obtain your most current information for your specific areas of expertise.

So we're going to actually, your first stop should be your security manager or your program or project office, because if you have classified information you should also have that security classification guide that goes along with it, and this really holds true for contractors out there working on classified contracts. The Defense Technical Information Center, or DTIC, does have an electronic index of classification guides. They do have the most current classification guides out there. All guides should be updated every five years, so if you're working with a classification guide and it's been dated back in the 1990s or the 2000s your guide is totally out of date and you need to have an updated guide. So if you can't find your guide at DTIC, your security manager can't really help you, then you really need to seek assistance from your higher headquarters or go above your agency to find your guide.

Initial access one of the other requirements is marking. As a derivative classifier, as an OCA, you need to be familiar with the marking requirements and you know how information is classified, decisions that OCAs make. More expressly, all of this list of sources that you're using to do derivative classification. If you go to DoD Manual 5200.01, Volume 2, that has all the information you could possibly need in there for how to properly mark classification as well as trying to avoid over classifying pieces of information. CDSE has got marking in the e-learning format, we have downloadable job aids, we have marking shorts that are out on our website, so we have a bunch of information that you can go out there and take a look at and use for your security training. Some additional requirements are specifically when we talk about control markings if you don't know what a control marking is, control markings are really used to limit or expand distribution of classified pieces of information such as, releasable to certain agencies or countries, or not releasable to, so you need to be familiar with those dissemination and control markings. Also how do you process information as it regards challenging classification decisions, if you think information has been over classified and you know that it should have been classified at a particular level, what outlets do you have and how do you go about that process. You can find all of that information as well in the manual. Also how to downgrade and declassify information is very important, because you might be the one that actually has to go through that process and specific requirements as it pertains to working papers, because working papers in themselves have specific rules that you need to be familiar with.

What you see on the screen now is one of our, another one of our wonderful posters and it's leading into security incidents. Security incidents, and I know this list that I'm going through seems like it's going to never end, but you really need to have the foundation for why it is so important to train your folks up on the policy requirements. One important item that's been in the news very, very frequently, one thing that we really need to be mindful of is being able to identify when a security violation is actually taking place or security incident. You need to train your folks on what qualifies as a security violation vice an infraction, and what compromises are and what an unauthorized disclosure mean. Disseminating classified information echoes along with saying because we share information, our classified information, with different states we share it with local, tribal, private sector officials, even some of our foreign governments, we share our classified information. This in itself really poses a significant risk that we need to make our individuals aware of when we're handling our classified information.

So let's take another poll question, poll question number 4 asks that, if you are authorized access to classified information systems, you should have additional training that is called which one of the ones you see on the screen? INFOSEC, OPSEC, Information Assurance (IA) Training, Physical Security Training. A lot of you are choosing Information Security Training, but the correct answer for this one is Information Assurance Training. I'm going to tell you why. We have what's called DoD Directive 8570.01 which governs Information Assurance training, certification, and workforce management, and that regulation requires that Information Assurance training is accomplished for all personnel who are authorized access to classified information systems. Requirements are also found in the DoD Manual 01, which has specific requirements as well. Those requirements really revolve around the use of information systems for creating documents in the electronic environment, storing information, as well as processing and transmitting information, on those systems. And as you know if you have access to a classified system, we mark information in the electronic environment. We have documents, we have web based, we have databases, and even spreadsheets that have to be marked if it is on a classified system. We process information through our computer media, we use our floppy disk, we have cd's and dvd's, even classified removable data storage, so we need to make sure that we have the proper training in all of these areas. We need our training because if an unauthorized disclosure of classified information occurs on your system or network, typically known as a data spill, we need to know the process to be able to handle that.

So one of the chat questions I'd like to ask as we continue on this is, can you identify quickly for me some situations that may require special training requirements? If you go ahead and type in that little chat box that I initially talked about, we'll see some of your information populating on the screen and I see that some of you talk about NATO, hand carrying requires special requirements, COMSEC, very good you guys are on the ball with this today. So just to outline some of those special training requirements, you can see them listed here on the screen. What you also see is a deployable security trainer. What this is, is a job aid that is downloadable, we have it out on our CDSE website, and it does address a lot of these special training requirements,

it has quite a bit of information from the DoD Manual from all of the volumes that really goes into detail about a lot of information that a security manager or security specialist that has deployed would need to have handy. So make sure you when you get a chance to take a look at that website, I think we have a link at the end of the webinar that will kind of link you to that. But just be mindful that if you travel over the foreign countries, if you have any courier duties specifically or if you have access to special types of information such as SAP or SCI or NATO, or even if you work with international programs, or foreign government information, that you will be required to have a special type of briefing.

To flip the script a little bit I want to highlight OCA training here. Some of you, if you're in the position you might be responsible for providing training to your OCAs, if you have any of them, and OCAs must have all of the training requirements that are specified here. If you go to the DoD Manual, Volume 3, Enclosure 5, which we've provided you a copy of, you can see all the specific training requirements for an OCA and they are a lot of the same training requirements that are in your initial orientation. The classification authorities, they are very similar to original classifiers but not original classifiers, they primarily have the responsibility of going through declassifying information but they need to know the standards and methods for how to declassify, create, declassification guides they have to be familiar with your local DoD components declassification plan if they have one, and their also required to have what is called a declassification database. Addressing information as it pertains to mandatory requests for declassification of information that is primarily the responsibility of a declassification authority, and they too also have to have training which is specified as you see on the screen in Enclosure 5, Section 6.

Annual Refresher Training is mandated, I know as much as we stay busy all the time, and we always have to stop and take this course and that course, when you have annual refresher training because it's mandated, it really reinforces what I like to call the 3 "P's" which is your policies, the principles of information security, and your procedures because sometimes procedures do change if they're not working. So you have to do a review of all of that information and again that's to all personnel that have access to classified information. But there's a couple items that specifically pertain to refresher training that has to be addressed, and that is the threats and techniques that foreign intelligence agencies use because they constantly change as well, you have to notify individuals of their penalties, again folks need a reminder that there are consequences for engaging in espionage activities or any other unauthorized disclosure. Refresher training also has to address any relevant changes in policy, if you've done your component self-inspection, and you've noticed issues or you have concerns within your own areas, this is a good time to provide refresher training on how to go about correcting these items of concern.

So this is just a slide to really give you the outline the training requirements for OCAs, and I mentioned earlier that they must be trained annually. Derivative classifiers and declassification authorities require training every two years. If you do the training please make sure that you

track the training because if you don't track it, you might as well say that it hasn't been done. We need to do our due diligence as good managers and it only makes sense to track your training.

So what you see here is a little excerpt that says read and initial. I know a lot of times we use the read and initial method in conducting our training, but just be mindful, you can use it but it cannot be the only method that you use to conduct our education and training. As you go through and do your periodic briefings, your training sessions, you need to try and incorporate other information and promotional efforts to make sure that your training is providing a continuing awareness, and that it is also promoting that quality performance that we talked about a little bit earlier. So read and initial has its place, but it cannot be a stand-alone method for training.

Termination briefing, just when you think you might be free and clear to do or say what you want you might just want to think again, because just because you are leaving the cleared community or maybe a particular classified program, you are not absolved of your responsibility to protect classified information. Those cleared employees who leave the organization, or even if your clearance is terminated, you have to receive a termination briefing. You have to be reminded that you have a continued responsibility to protect your national security information. You also need to be reminded that if you provide any of our classified information to anyone that's not eligible to have that information, you're committing an unauthorized disclosure of that and you are still subject to the civil and criminal penalties that are out there. So you really need to be mindful of that. In addition, if you are retired personnel, if you're a former DoD employee, or even a non-active duty member of any of the reserved components, anything that you submitted in writing, like if you're going to write a book about any information that may have been potentially classified previously, anything that you write or you have to submit that writing and any other material for DoD security review, before any of that information can actually be released to the public.

And lastly, the few things I want to highlight here pertaining to managers. If you are a security manager, if you have classification management, office of authority or security specialist, or even if your duties significantly involve managing and overseeing in any classified information security programs, you need to know all of these training requirements that we see here on the screen. That means the same training that's required for derivative classifiers, you have to have it because if you don't have it, if you don't know what the policies say, how can you appropriately perform adequate oversight and management. So you need to know what these items say here. If you go to Enclosure 5, Section 10, it does outline additional management and oversight training requirements. And again this goes back to we talked about that IA training, certification and accreditation of networks, well if you are in that environment and you have classified networks or classified systems, you need to know the process to get those systems certified and accredited to make sure that you remain in compliance. Also declassification reviews, well you might be the one responsible or you might be the one that actually get those

reviews or have to have that information coming to your office, so you need to know what to do with it.

Program oversight and self-inspections, again mandated every year, annual basis, your self-inspection should be done. You should use that opportunity to be able to clear out some of your information that you don't need, to go through your classified policies or procedures. And also to look and do an inspection of a certain percentage of your derivative classification products that you've created, which is also another requirement.

And lastly, I'd just like to really highlight that if you are conducting any type of program or oversigh,t and even if you're not, you really all need to be part of the solution and not part of the problem. When you are conducting training, just remember that your training must be evaluated, training records must be maintained for all of your training, and when you're doing it you need to be accessing quality and the effectiveness of your training and making sure you are reaching the appropriate target population. So that's really all the information I have this afternoon on security education requirements.

And lastly if you'll just look at this slide it does have our contacts and resources and all of this information does link out to our website for those job aids and webinars we kind of talked about. So I would just like to thank everybody for attending this session this afternoon and hope you all have a fantastic weekend.