SECURITY INCIDENT REQUIREMENTS

March 21, 2013 Webinar

Welcome and thank you for standing by. For the duration of today's conference, all parties will be able to listen only. Today's conference is also being recorded. If you have any objections please disconnect at this time. And I'd like to turn the call over to your host today, Ms. Lisa Rainey. Ma'am, you may begin.

Before we get started this morning, please be aware that the video portion of this webinar is being recorded. Once the red recording light appears we will begin. So, good afternoon everyone, my name is Lisa Rainey and I will be your host for the next 30 minutes, and I do really appreciate everyone taking time out of your busy schedule this morning to go ahead and receive this piece of information again in our Information Security webinar series. And today's topic is on Security Incident Requirements. But as usual, I always like to start off with getting individuals that are new to the webinar series familiar with our administrative announcements, as well as our Q&A box and how that works.

So if you go ahead and take a look at the screen you will see what is called a Q&A box which is kind of in the center of the screen. That box is for you to be able to submit questions and be able to respond to some of our poll questions that we may submit to you. And this morning we do have a large number of participants and we might not be able to answer all the questions that are submitted during that webinar, but do not worry, because we will have your questions all answered and posted in our Frequently Asked Questions, or FAQs location which is under the same area where you found the descriptions for the webinar today. So if you go ahead and look at your screen on the bottom left corner you will see what is called a File Share box. In that box we provided for you today a copy of our webinar presentation which you can download and print, take notes as you like as we go through the presentation, and we've also enclosed for you a copy of Enclosure 6 of the DoD Manual, Volume 3, from which we're going to be pulling most of the information today as well, and you can use that for additional policy guidance related to our main points of discussion today. So as we go through the webinar, you're going to notice that questions will appear on the screen periodically and kind of randomly, and these are poll questions and they generally just help me to do a little check on the information that we're presenting to you and see what you know about the questions that we're asking. And as such, having said that, I do like to always start off with a poll question just so you can get the feel for how they actually do work.

So our first poll question for today does ask, where can you find information regarding security incidents? And if you go ahead and select the proper answer, at least where you think you can find that information, you should be able to see on your screen as well all of the responses that we're getting and we do have 100 percent response for the correct answer today. Very good. So

DoD Manual 5200.01, Volume 3, Change 1, specifically Enclosure 6, really talks about security incidents. And that's where a lot of our information is going to come from today. So as I said already, the DoD Manual, Volume 3, Enclosure 6, specifically talks about security incidents that involve classified information. As most of us or all of us are probably security professionals that have access to classified information, we should have all been briefed that protection of our classified information is essential. So how we maintain our security and our operational on war fighting environments and as well as achieving our mission success, and as such we do have a responsibility to make sure we are promptly reporting any security incidents to ensure that these incidents have been properly investigated, as well as making sure we're taking the necessary actions to be able to negate or minimize the adverse effects of an actual loss or an unauthorized disclosure of our classified information. The one important thing we want to try and do is make sure we preclude recurrence through having an informed and properly tailored, as well as an up-to-date security education and awareness program, which is very important.

In some cases where we know our compromise's actually been ruled out, and there's been no adverse effect on national security, we always like to try to take a common sense approach to early resolution of that incident, and specifically at the lowest appropriate level. All security incidents involving classified information compromises or loss, they do have to involve at least an inquiry and investigation, or sometimes they may have to have both of them depending on the nature of the situation. So I'm going to define for you the difference between a compromise and actually a loss.

So when we have a compromise, it is a security incident, and, more specifically, a violation in which there is an unauthorized disclosure of classified information generally a disclosure to a person who does not have a valid clearance; they do not have authorized access nor do they have a need to know. A loss, on the other hand, basically occurs when classified information cannot be physically located or even accounted for, and generally we find this out doing some sort of an audit or if we're doing our self- inspections and we're looking for some information and it cannot be readily located. So, this is a chat question for you and it does ask: When would a security incident require an investigation? And for this one in your chat box at the bottom I need for you to go ahead and type in some responses of when you think and a security incident would require an investigation. Waiting for some of those responses. Some of you are saying always, when there's a loss, when there's a violation, and these are very, very good answers because a security incident does require an investigation if an actual compromise or loss of information has actually occurred. You guys are on the ball with these responses coming in here. Thank you so much again.

So we're going to go ahead and move on to security violations just to be able to define the differences here between a violation and infractions. When we talk about security violations, they are incidents in which knowing willful or negligence of security policies have resulted in, or could be expected to, result in the loss or compromise of classified information. And some of those examples of violations would fall under any types of unauthorized disclosure of our

classified information, if we misclassify information or classify it incorrectly, the continuance or the discontinuance of a SAP, and anything else specifically outside of the requirements of the manual that doesn't fall under the realm of an infraction and it actually, like I said before has to result, and it could be expected to result, in a compromise. And like I said earlier, it requires an inquiry and it may require an investigation or even both. Security infractions, on the other hand, is an incident involving a failure to comply with the requirements of the manual or even any other security policy which cannot be reasonably expected to, and it does not result in the loss or suspected compromise of classified information. When we have infractions they're generally either unintentionally, sometimes they're accidental or inadvertent, and while it doesn't constitute a security violation, if these practices are left uncorrected they can lead to security violations or even compromises. These security infractions do require an inquiry as well at least facilitate immediate corrective action, but they do not require an in-depth investigation.

Talk a little bit about inquiries specifically. When we talk about an inquiry, what they are is actually a fact finding analysis, and that's conducted to determine whether or not there was a loss of compromise, excuse me, a loss of classified information or whether or not an authorized personnel had or could have had access to the information. When you do an inquiry you're really looking to identify the facts of the situation, you're really trying to characterize the incident as either an infraction or violation. You want to identify the possible causes of what the whole situation was revolving of why it happened, and any persons may be or are responsible. You also want to make sure that you report corrective actions taken, or actions to be taken, as well as making recommendations as to the need for any further corrective action or even a more in-depth investigation. And like I said before, we want to always try to make sure that these inquiries are initiated and conducted at the lowest possible level within your components or even your agencies.

When we do an investigation, these are done for security violations when the incident cannot be resolved by way of an inquiry, and also for incidents where you know that an in-depth and comprehensive examination of whatever that case may be is more appropriate, or a better approach.

Some security tips I like to kind of throw these out there, because I know we have practices within our agencies that are not always the best practices and some of these tidbits to remember, that like I said before is that certain practices dangerous to security even though they may not be reportable as security incidents, some of them do have the potential to jeopardize your security of your information, and material if you allow them to perpetuate. And some of these practices that we use which are really not good practices are placing a paper or a recycling box maybe next to a classified copier. In some cases, we place burn bags next to unclassified trash cans, which is a very bad practice, and even stopping at public establishments to conduct our personal business sometimes while we are hand carrying classified information and we know that is totally unacceptable, or even failing to change our security container combination when we're supposed to. These practices again, when they are identified, you want to be able to address them, at least

security management should address them and make the appropriate changes and take any actions or even provide training as necessary to make sure that everyone understands how a classified information is supposed to be secured. So let's do another poll question.

Poll question number 2: It asks you to select any of the following that are dangerous security practices. Just want to make sure that you all are still awake out there, I know it's early, it's almost lunch time, when you're done with me you can gladly go have lunch. Some of you may already be having lunch. So some of the correct answers that we have here is answer A: recycling box next to a copier, trash can next to a burn bag, personal business doing hand carrying, and even storing a combination in an unapproved container. And again these are just some of the examples, the list is totally not all conclusive, because I'm sure there are other practices out there that occur that may be dangerous practices.

Let's talk a little about consequences of compromise of our information. Generally, these compromises of classified information, when it occurs, they really threaten our national security, and they can also damage intelligence and operational capabilities that we have. But it also lessens our ability to be able to protect our critical information, our technologies and even our programs, and it does reduce the effectiveness of our Department of Defense management. But once a compromise is known to have occurred, the seriousness of the damage or even the extent of that adverse effect on national security must be determined, and we have to be able to take in those appropriate measures to be able to minimize any adverse effect. When possible, actions must be taken to be able to regain custody of documents or materials that was compromised, but in all cases management must take action to identify the source and the reason for that suspected or actual compromise and take remedial action to prevent it from reoccurring.

This is very important and when we talk about reporting and notification process, I know all of us depending on the agencies that we're in and where we work whether you're a DoD civilian, you might be a contractor, you may be active duty reservist or even national guard, but anyone who finds classified information out of proper control must immediately take custody of that information and safeguard that material. As well as notifying your appropriate security authorities and I know the regulation says by secure communications when it is available, that is the preferred method, and if it is not available you need to use whatever means necessary to make sure that the proper authorities are notified. If the person that found that information believes that the head of the activity or even the security manager may have been involved or responsible for that incident, they have the right to report it to the security authorities at the next highest level within your command or even within your supervisory chain. When we report confirmed security incidents or the confirmed incidents actually do have to be reported to the Director of Security for the Office of Under Secretary of Defense for Intelligence, also known as USD(I), that is necessary when these incidents have significant consequences or the fact of that incident may become public. We also have to notify USD(I) for any cases that may potentially involve espionage; any types of unauthorized disclosure of classified information that may be in the public media, but there is a caveat to that public media statement. And it's that if any

additional notification, excuse me that additional notification is actually not required, for reference to or re-publication of a previously identified media disclosure, so if it's already been identified or if it's already been reported, it's not required to be reported again to USD(I).

Some of those other violations are the continuance or creation of a special access program, any of those security failures or compromise of classified that relates to again, defense operations, systems, or technologies that might cause significant harm or damage or even damage our national security interest. Some additional reporting requirements is that anytime there's an unauthorized disclosure of classified information, if violations are reportable to the oversight committees of Congress, anytime a violation may attract significant public attention, if it involves large amounts of classified information but also if it reveals potential systemic weakness in our classification safeguarding and de-classification policy or practices, or if there's policy out there that actually causes these violations to occur, these things have to be reported and we have to be able to take appropriate action to be able to get them resolved. Question was asked, do we have to classify incident reports? Well, incident reports are required to be classified according to the content of that report and at the prescribed level by your applicable security classification guide. But at a minimum, reports have to be designated FOUO and marked as required by the DoD Manual, Volume 4, which talks about CUI, or controlled unclassified information. And that's required in order to provide the appropriate protection for that inquiry and for information regarding personnel involved in information that could facilitate in unauthorized access.

If the information, if the loss or compromise information is beyond the jurisdiction of the government and that information cannot be recovered, such as if it was in a media link or a public website post, or even in a foreign country, then the report and location of that compromise must be classified in accordance with the classification level of the material to prevent any further unauthorized disclosure. If the FOUO report is to be shared or disseminated outside the Department of Defense, you have to put on the face of the document a marking or statement that specifies that the information may be exempt from mandatory disclosure in accordance with the Freedom of Information Act, or FOIA.

What you see on your screen here is a report of security incidents inquiry of investigation, and this is just a sample that's provided for you as well in the manual, it's Figure 2, this is not mandated that you use this format but it is provided because it's kind of a thorough template for you to be able to use to be able to go through your inquiry and make sure that all areas are actually taken and that everything is actually covered. We have provided a copy of that as well in your file share box, you can use it if you like but DoD Manual has provided that for you.

Suspicion of Criminal Activity, this really talks about when information suggestive of a criminal or a counterintelligence nature is actually discovered, that all actions that's associated with that specific inquiry or investigation, must cease pending coordination with the DCIO having oversight or even with the Defense CI component that has oversight. If the DCIO or that CI

component accepts the jurisdiction, then the inquiry must not be resumed without their agreement. Any relevant information must be released with the annotation in the report that the matter was referred to the specific DCIO or even to the CI component, and after coordination with both of those agencies, the OCA must be notified and any others that may be involved with this particular inquiry. But if the DCIO or the CI component declines jurisdiction over this piece of information, the security inquiry or the investigation actually continues, but it has to be annotated as well on the report with the identity of the official who made the declination decision and the organization that they belong to. If any inquiries or investigation determines that a compromise actually occurred, then the person that's initiating that inquiry has to immediately notify the originator or the OCA of that information that was involved. There are some specifics that pertain to this notification process and that's if the originating activity is no longer in existence, then the activity that actually inherited those functions of the originating activity has to be notified. And if those functions were actually dispersed to more than one activity, or more than one activity actually has equities in that information, or if the agency cannot be determined or even if the functions have ceased to exist, then you would basically notify whoever the senior agency official is of the originating activity for which that information was a part of.

But of course we will not delay this notification, pending completion of any additional inquiries or investigations or resolutions of any other related issues to that specific inquiry.

Let's talk about our timeframe, as it pertains to how long we have to get these inquiries done. So if there is an inquiry into an actual potential compromise and as we said before, these inquiries are done to determine the facts and the circumstances of the incident, and to also characterize that incident as an infraction or a violation. At the conclusion of the inquiry a narrative of all those findings have to be provided in support of the recommended additional investigation, or any other actions that might be recommended by the activity. When we talk about who's responsible for doing that, the person that is appointed to lead the inquiry cannot be anyone involved with the incident, and it is preferred that the security manager not be appointed to lead that inquiry and I know sometimes that's always not the case, and there has to be extenuating circumstances as to why the security manager is the one that's actually leading the inquiry. This inquiry must be initiated and completed as soon as possible not to exceed 10 duty days, very specific. And a report of those findings must be provided to the activity head, to the activity security manager and anyone else who's involved as appropriate. But if that inquiry cannot be completed within those 10 duty days, that person that's doing the investigation has to request an extension to that appointing official. So it's very important that we try to adhere to that 10 duty because it is mandated in the manual.

Some additional responsibilities are that any recommendation regarding punitive actions or sanctions cannot be made by that inquiry officer, more specifically, like I said their function is to determine and report the facts and make those recommendations for any actions needed to prevent any future violation. Disciplinary or any punitive action is the responsibility of that appropriate military commander, or the overseen management official, not that security manager.

But if the results of that inquiry are sufficient to provide all the necessary answers, then the information should be considered sufficient to be able to resolve the incident, as well as including any administrative sanctions that might have been recommended or even imposed. So when we have to do a security investigation, this is when the circumstances of that inquiry requires a more detailed or even an additional investigation, that individual that is appointed, must be appointed by the activity head in writing to be able to conduct that investigation, and they also have to provide recommendations for any corrective or disciplinary actions. The person that's appointed has to be sufficiently senior and that's to ensure that a successful completion of the investigation actually occurs, and that their rank should really be commiserate with the seriousness of the incident. An example is generally you're not going to have a GS-2 do a security investigation that really involves a bunch of GS-13s and GS-14s. You want to try and have that rank sufficiently commiserate. And that person also has to have an appropriate security clearance. They need to have the ability to be able to conduct an effective investigation and also be unlikely to have been involved or directly or indirectly in the incident.

Again in unusual circumstances that security manager will not be appointed unless absolutely necessary to conduct that investigation. And because that investigation may lead to administrative or disciplinary action, you really want to make sure that the evidence that's developed is very comprehensive in nature and that it's gathered in such a manner that would be admissible in a legal administrative proceeding. If you're not sure or you need some guidance, you can always consult your legal counsel to assist you with how to proceed for conducting an investigation and to ensure that that information is admissible in a court of law.

So information appearing in the public media. If this actually occurs, including on those public internet websites, or even if you're approached by a representative of the media and you are DoD personnel you have to be careful not to make any statement or any comments that actually confirms the accuracy of or even verifies information that requires protection, you have to immediately report that matter as instructed by your own appropriate DoD component guidance, but do not discuss it with anyone who does not in the case of our classified information, have an appropriate security clearance, or even a need to know. If the fact of that unauthorized public disclosure becomes widely known, as we've kind of seen in the past, your component generally your senior agency official is the one who considers whether you all within your agency or organization needs to be reminded of those actions to be or not taken in response to this information once it's been disclosed. So really just follow what your component guidance is, DoD generally sends down information and that is filtered out to the agencies on how to respond appropriately.

So I want to talk a little about the results of inquiries and investigations and how we're supposed to handle these. If the conclusion of your inquiry or your investigation shows that a potential or actual compromise did occur, and that a weakness of vulnerability in your established security practices contributed to that compromise, then the appropriate security official has to take prompt action to issue new guidance and even to resolve those identified deficiencies, so your

security official has to make sure that they are addressing that and they're doing something about it. All results of inquiries and investigations into those actual potential compromises, that does indicate a defect in the procedures and the requirements of the manual contributed to the incident, that has to be reported to OUSD(I) for intelligence the Director of Security. If the conclusion of your inquiry showed that a compromise did not occur, but that there was a potential for compromise of your classified information, again due to a failure of individuals complying with those established security practices and procedures, then again that security official that's responsible for those persons also has to be responsible for taking the action as appropriate to be able to resolve that incident. In some cases, again those investigations may have to go beyond what is actually required by the enclosure. They may need to be or actually have to do that in order to allow additional application of the appropriate sanctions specifically for any violations of those regulations that involve criminal prosecution and even to determine an effective remedy for discovered vulnerabilities. So whatever the case is, you have to be able to be able to mitigate it, you have to apply the appropriate sanctions and any criminal prosecution necessary depending on the severity of that incident.

So let's do another poll question. And that poll question asks, the inquiry lead must complete a report in how many days? We kind of covered this information, I just want to make sure that you all remember that. And it looks like the majority of you or all of you have selected the correct answer. 100 percent the answer is 10 days. Very good!

Okay, compromises involving more than one agency and as I mentioned, this I think a little bit earlier that you will have agencies with equities and the same kinds of information, but if there is more than one DoD component or Federal agency involved all of those activities are responsible for collaborating their efforts and making sure that they evaluate the classification of that information involved to perform a proper damage assessment. Make sure you're getting input from all of those equities.

Debriefing in cases of unauthorized access. In those specific cases it may be advisable in some instances to discuss that situation with the individual and that's really done to enhance the probability that they will protect the information. And again that responsibility falls under the activity head and they basically determine if a debriefing is actually warranted or not. If you are debriefing an individual you want to really try to make sure that you have them acknowledge of their understanding and the responsibility of that classified information and what it contains and how it actually affects national security. You also want to make sure that you get an SF 312, which is our non-disclosure agreement signed. If that person refuses to sign that acknowledgement of that debriefing, you have to include that specific fact as well in your inquiry and your report for the results.

If you don't execute a non-disclosure agreement, then the nature in the format of however you develop your statement, it is left up to your discretion. It really allows you some flexibility and how you meet that need, so however you do it, whatever you document it on, you always want to

make sure that you're covering your information as much as possible and that that information is included as part of your report.

Reporting and Oversight Mechanisms- This is really important. This really just kind of outlines the reasons behind why we do these reports and the oversights that's required. All individual components are responsible for making sure that they provide timely and efficient reporting and oversight mechanisms; to make sure that the action and the appropriate actions are taken to correct any problems that are identified, whether they're deficiencies or incidents. Together the incident results and the analysis that management conducts, has to consider any possible systemic shortcomings that may have caused or contributed to the incident happening. Determining the causes and contributing factors to these incidents are really based on evaluating the effectiveness of your activity security procedures, the security education that you're providing, and what kind of supervisory oversight of your security practices you have within your agency. Management's main focus and response to these security incidents is to eliminate or minimize the probability of these incidents continually occurring. And lastly, simple disciplinary action without consideration of what other factors may have contributed to your situation or your incidents may not be considered an acceptable response to a security incident. So you really need to look at the whole situation.

You need to evaluate all of your policies and programs and procedures and even the security awareness status of your agency and organization to see if there are things that you are doing incorrectly or that you might need to approve upon within your agency. So really this is the gist of the information that we have here for you today. I do want to let you all know out there that we are in the process of having a new short on Security Incident Reports and Requirements uploaded and that should be done sometime in the near future. Hopefully by the end of the month, you should look out for that. We do have the links that are provided here for you of our webinars that we have conducted. This webinar will be posted up in just a few days, you'll be able to access it and share it and we will have webinars for the next couple of months actually that will continue within the security incidents series. The next couple of ones we're going to have will actually be talking about the special categories of information and how those incidents are supposed to be reported. We do have our next webinar that's coming up on ACCMs is going to be our next webinar which is going to be on April 18 and I hope you all can join us then for that webinar. So thank you very much, if you do have additional questions for the Q&A, please make sure that you go ahead and submit them in the box, and we will capture all those questions and get your answers posted up to our FAQ site as soon as possible. So thank you all and enjoy the rest of your day.