Information Security Continuous Monitoring

Webinar guests submitted several questions before and during the **December 4, 2014 Information Security Continuous Monitoring** session. The following responses are provided by the Center for Development of Security Excellence (CDSE):

Question: How is training as a Security Specialist being developed to incorporate IT/Cybersecurity workforce knowledge?

Answer: Right here at CDSE we are developing training designed for DoD 080 and contractor security personnel to enhance their knowledge of Cyber and IT. DoD has developed a cyberspace workforce strategy and it is loosely based on the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) framework, which discusses all of the functional areas required to effect good cybersecurity and specific training and education for each category. It is available for free download and worth checking out.

Question: Is there a listing of information security sources, that can provide guidance for employees on the following: cyber security, protection against data theft, and related topics?

Answer: Yes. CDSE provides toolkits which aggregate this information. Please see our website for the Cybersecurity Professionals and Information System Security Managers Toolkits, which have policy and tons of resources. Also, check out our Insider Threat Professionals Toolkit (which has a cyber-segment, as does the counterintelligence portion of the FSO Toolkit).

Question: We have a TCP & ECP since we are under FOCI so many of these ISCM items are already being monitored.
Answer: That great to know that you have a Technology Control Plan and Export Control Plan. It is also a great idea to include these as a part of your ISCM strategy.

Question: Is there a cleansing procedure being worked on for iPhones, similar to the Blackberries, involved in data spills?

Answer: I know that Apple's iOS 6 mobile operating system was approved for government use; however, I am unaware of a specific policy governing cleansing procedure in case of a data spill. Again, I will point you to the NIST publications as they would be the authorities.

Question: Are there templates and/or sample documents available for ISCM strategy and programs?

Answer: The best place to find assistance with setting up your strategies, tools, guidelines, etc. is to refer to the NIST publications.