Q1: There are many security configuration documents on the Web, where is the best place to start?

Answer:

If NIST has not produced a guide for a specific product, federal agencies should browse the National Vulnerability Database and look at the National Checklist Program Repository to select a government-developed guide (such as Defense Information Systems Agency or National Security Agency) or a vendor's guide that they could use as a baseline. When such security configuration guides do not exist, federal agencies may carefully select third-party produced guides. Regardless which guide is selected, it is recommended that federal agencies document how their deployed information technology products are secured or deviate from the recommended checklists.

Q2: I know DoD has replaced DIACAP with the NIST Risk Management Framework but where can I learn more about RMF requirements?

Answer:

CDSE offers several courses on Risk Management Framework in our online learning management system called STEPP. These courses cover everything from a basic overview to detailed explanations of RMF's 6 – Step Procedures. You can access STEPP from www.CDSE.edu.

Q3: Who is subject to FISMA, and what is required?

Answer:

The Federal Information Security Management Act applies to agencies within the federal government. Under the act, these agencies must maintain a program that provides security for information and compliance systems that support their operations. CIOs, program officials and inspectors general at the agencies are required to conduct a yearly review of the program and submit the results to the Office of Management and Budget (OMB).

Minimum security requirements and controls spelled out by NIST are considered a starting point for agencies in choosing appropriate controls. Except where the OMB says otherwise, agencies have considerable flexibility in how they apply NIST guidelines. This flexibility has led to very different security regimes at different agencies.

Q4: Is the use of encryption mandatory in the HIPAA Security Rule?

Answer:

Surprisingly the answer is, No. According to the U.S. Department of Health & Human Services (HHS) final Security Rule, the use of encryption is an "addressable implementation specification". After a risk assessment, the entity can determined if the use of encryption is a reasonable and appropriate for safeguarding the confidentiality, integrity and availability of Electronic Protected Health Information (e-PHI). If the entity decides that encryption is NOT reasonable and appropriate, then they must document what equivalent alternative measure, was implemented along with the rationale for this decision. [Ref: 45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii)]