

Session S22 – The Federal Perspective on Information Security Governance

By Mike Nelson, SecureNet Technologies

Topic Summary

This session will provide a high-level overview of the family of National Institute of Standards and Technology (NIST) IT Security documentation and explores how they can be applied to fit the specific needs of State, Regional, Local agencies and private sector companies. NIST, part of the Technology Administration of the US Department of Commerce is playing a critical role in defining and documenting the concepts, standards, processes and techniques designed to ensure adequate protection of Information Systems. In the Federal Information Systems Management Act of 2002, Congress chartered NIST with developing the definitive set of Information Systems Security controls and processes and made the application of those processes mandatory for Federal Agencies. Key to the successful implementation of the NIST program is a clear understanding of the various roles that play a part in the risk management process. We review each role and discuss its inputs, outputs, responsibilities and authorities. We also gain a thorough understanding of the requirements and processes to formally certify and accredit an Information System to operate – the key to Information Security Assurance.