Title of Panel: *GUIDELINE FOR IMPLEMENTING CRYPTOGRAPHY IN THE FEDERAL GOVERNMENT*

Panel Presenter: Annabelle Lee, National Institute of Standards and Technology (NIST)

Session Abstract and Panel Position Statements:

In today's world, both private and public sectors depend upon information technology systems to perform essential and mission-critical functions. In the current environment of increasingly open and interconnected systems and networks, network and data security are essential for the optimum use of this information technology. For example, systems that carry out electronic financial transactions and electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data.

Cryptography should be considered for data that is sensitive, has a high value, or represents a high value if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. Cryptographic methods provide important functionality to protect against intentional and accidental compromise and alteration of data. These methods support communications security by encrypting the communication prior to transmission and decrypting it at receipt. These methods also provide file/data security by encrypting the data prior to placement on a storage medium and decrypting it after retrieval from the storage medium.

The purpose of the *Guideline for Implementing Cryptography in the Federal Government* (SP 800-21) (hereafter referred to as *The Guideline*) is to provide guidance to Federal agencies on how to select cryptographic controls for protecting Sensitive Unclassified information. *The Guideline* focuses on Federal standards documented in Federal Information Processing Standards Publications (FIPS PUBs) and the cryptographic modules and algorithms that are validated against these standards. However, to provide additional information, other standards organizations, (e.g., American National Standards Institute (ANSI) and International Organization for Standardization (ISO)) are briefly discussed. This guideline was written for federal employees who are responsible for designing systems, and procuring, installing, and operating security products to meet identified security requirements. This guideline provides information on selecting cryptographic services and methods and implementing the methods in new or existing systems. The purpose of the presentation is to provide an overview of this guideline.

Point of Contact Information and Biography:

Annabelle Lee, NIST
301.975.2941 (phone)
301.948.1233 (fax)
annabelle.lee@nist.gov

Ms. Lee has over 25 years experience in Information Systems. Prior to working at NIST, Ms. Lee worked for the Mitre Corporation as a Lead Engineer in the Criminal Justice and Public Safety Division. She provided support to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division and the El Paso Intelligence Center (EPIC) Information System (EIS) for the Drug Enforcement Administration. She was also author and co-author of documents in the "rainbow" series, the security standard for the federal Government. Currently, Ms. Lee is a Computer Specialist in the Information Technology Laboratory, Computer Security Division. Ms. Lee supports the Cryptographic Module Validation Program (CMVP) serving as the primary point of contact for three of the four testing laboratories. She also is the technical lead for the update of FIPS 140-1, *Security Requirements for Cryptographic Modules*. In addition, Ms. Lee recently authored the *Guideline for Implementing Cryptography in the Federal Government*.