Seeking a National Standard for Security:

Developing a Systematic Crosswalk of the Final HIPAA Security Rule, the NIST SP-800-37, NIST SP 800-53 Security Guidelines (TBR), ISO 17799, etc.

Lisa A. Gallagher, Senior Vice President
URAC I&T Accreditations
March 2003

URAC

Background

- **NIST**
- **URAC**
- **VA Standards and Tools**
- **NIST/URAC Health Care Security Certification & Accreditation Workgroup**

NIST and Information Security

The mission of NIST's Computer Security Division is to improve information systems security by:

- **Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;**
- **Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;**
- **Developing standards, metrics, tests and validation programs:**
  - **to promote, measure, and validate security in systems and services,**
  - **to educate consumers, and**
  - **to establish minimum security requirements for Federal systems**
- **Developing guidance to increase secure IT planning, implementation, management and operation.**

URAC

URAC

- **URAC is a nonprofit, charitable organization founded in 1990 by various stakeholders in the health care community.**

- **URAC's mission is to promote greater consistency and uniformity in health care operations through accreditation programs, educational workshops, research and publications.**

- **Recent Work in Security**
  - **NIST/URAC HC Security C&A Workgroup**
  - **(Draft) HIPAA Security Accreditation for CEs and BAs**

URAC

NIST/URAC Health Care Security Certification & Accreditation WG

Mission

- **Bring together key stakeholders from the public and private sectors to facilitate communication and consensus on best practices for information security in healthcare.**
- **Promote the implementation of a uniform approach to security practices and assessments by developing white papers and crosswalks, and provide educational programs, as appropriate.**

Goals

- **Review NIST Special Publications 800-37 and 800-53 for possible use in the healthcare sector.**
- **Review other security standards such as the HIPAA Security Rule, ISO 17799, CMS' CAST requirements, Systems Security Engineering Capability Maturity Model (SSECMM), CMS Internet Security Requirements, among other possible requirements or standards.**
- **Develop a common set of health care security standards that will cover security policies, procedures, controls and auditing practices.**

URAC

ISO

- The **International Organization for Standardization (ISO)** is a worldwide federation of national standards bodies from more than 140 countries.
- ISO's work results in international agreements which are published as International Standards.
- Similarly, the **International Electrotechnical Commission (IEC)** prepares and publishes international standards for all electrical, electronic and related technologies.

URAC

VA

- **VA Office of Cyber Security, Center for Healthcare Information Security**
- **VA consolidated Cyber Security staff**
- **Responsible for cyber security initiatives to protect VA's IT assets**
- **Internal Directives and Policies**
- **Federal Government Regulations, Standards and Guidelines**

URAC

Panel of Speakers

- **Dr. Ron Ross, Ph.D., Director, Computer Security Division, NIST**

  Topic: Assessing the Security of Federal Information Systems: The development of Standardized Certification and Accreditation Guidelines and Provider Organizations

- **Arnold Johnson, Manager, Security Certification & Accreditation Assessment Program, Computer Security Division, NIST**

  Topic: ISO/IEC 17799, Code of Practice for Information Security Management

- **Dennis M. Seymour, CISSP, Director, Center for Healthcare Information Security, VA Office of Cyber Security**

  Topic: VA Security Standards and Tools for Healthcare Security

URAC