Today’s Challenges in Cyber Space An Introduction to the Certification and Accreditation Process (C&A) Within the U.S. Government

Jeff Waldron, CISSP, SCSA

Artel Inc.

May 2004

Introduction

- Office of Management and Budget (OMB) Circular A-130 (February 8, 1996) requires federal agencies to plan for security and to further ensure it is reviewed during the life-cycle of an Automated Information System (AIS)
- This guidance was effective upon issuance of the Circular

Benefits of the C&A Process

- Provides more consistent, comparable, and repeatable methods for the C & A process for all federal agencies
- Provides better understanding of associated risks, vulnerabilities and counter-measures lessening the likelihood of legal action due to negligence
- Provides increased security awareness throughout the organization
- Provides a controlled configuration management facility to ensure greater uptime of IT systems
- Helps to reduce computer fraud and related crimes

Current C & A Within the Federal Government

- Defense Information Technology Security Certification and Accreditation Process (DITSCAP) – Department of Defense (DoD)
- National Information Assurance Certification and Accreditation Process (NIACAP) – Federal IT systems (non-DoD)
- Federal Information Processing Standards (FIPS) 102

Future C & A Within the Federal Government

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37
- Guidelines for the security certification and accreditation of federal information technology systems – federal IT systems

NIST SP 800-37

- Supercedes FIPS 102
- SP 800-37 is a development that attempts to streamline the security certification and accreditation process
- SP 800-37's goal is to develop a more efficient, less document-centric process when compared to the DITSCAP, NIACAP, and FIPS 102
- Redefines the phases in system development life cycle of an information system: (I) initiation Phase; (ii) security certification; (iii) security accreditation phase; (iv) continuous monitoring phase - operations and maintenance

Common Criteria for Information Technology Security Evaluations

- This is the National Information Assurance Partnership (NIAP)
- Can significantly reduce the cost of C & A by incorporating test and evaluation results
- Can assist agencies in deploying, operating and maintaining more secure IT systems
- Provides standardized evaluation criteria

SP 800-37 Certification and Accreditation Phases

- **Initiation Phase**
- **Security Certification Phase**
- **Security Accreditation Phase**
- **Continuous Monitoring Phase**

Questions?