TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

A presentation by
Lawrence Feinstein, CISSP

April 14, 2004

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Current Macro Security Context within the Federal Government

- Security engineering and information assurance are more important than ever before.
- A strong consensus has emerged that *electronic* attacks can compromise the national security interest of the United States every bit as much as *physical* attacks.
- The traditional gap between theory and practice has greatly narrowed.
- Over the past several years, security standards have been raised significantly and will likely become even more stringent in the future.
- Over the past several years, many major new security initiatives have been launched.
  - Across all Federal agencies and departments, examples include crackdowns in immigration policy, changes in airport procedures, and Homeland Defense.
  - Within the DoD sector, examples include the wars in Afghanistan and Iraq, the Common Access Card (CAC), and newly established restrictions regarding the use of vulnerable ports, protocols, and services (PPSs) in communications.
- Security considerations now impact every aspect of a system, including acquisition, budgeting, design, testing, deployment, and logistics.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

DITSCAP Basics

- DITSCAP is an acronym that stands for "DoD Information Technology Security Certification and Accreditation Process."
- DITSCAP is the prescribed DoD *methodology* for performing Certification and Accreditation (C&A) of a system.
- DITSCAP is intended to be a standardized "purple suit" approach to performing C&A efforts across the DoD sector.
- As a true *lifecycle* process, DITSCAP is applied *individually* and *repeatedly* against a specific DoD *production* system.
- A DoD production system is required to undergo a new baseline DITSCAP effort at least once every three years, or whenever it implements a "major change" within its underlying security model.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Major DITSCAP Activities

- The DITSCAP methodology is generally fulfilled by the following major activities:
  - Development of comprehensive security documentation.
  - Performance of rigorous system security testing.
  - Identification and remediation of security vulnerabilities (“hardening”).
  - Validation and review by one or more predetermined *independent* third parties.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Important DITSCAP References

- The basic process flow of the DITSCAP methodology is defined in DoD Instruction 5200.40, which was promulgated on December 30, 1997.
- Application guidance for the DITSCAP methodology is provided in DoD 8510.1-M, which was promulgated on July 31, 2000.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Why do we apply DITSCAP?

- DITSCAP provides the following benefits to a system:
  - Verification of the integrity and effectiveness of the underlying security model.
  - Assurance that all applicable security requirements, policies, standards, directives, and guidelines are addressed to the extent possible and practical.
  - Identification and mitigation of deployment risk.
- At the Federal level, C&A is mandated as a security control for all US government systems by OMB Circular A-130 (February 8, 1996).
- In the DoD sector, DITSCAP is mandated as the prescribed C&A methodology by DoD Instruction 5200.40 (December 30, 1997).

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

When do we do apply DITSCAP?

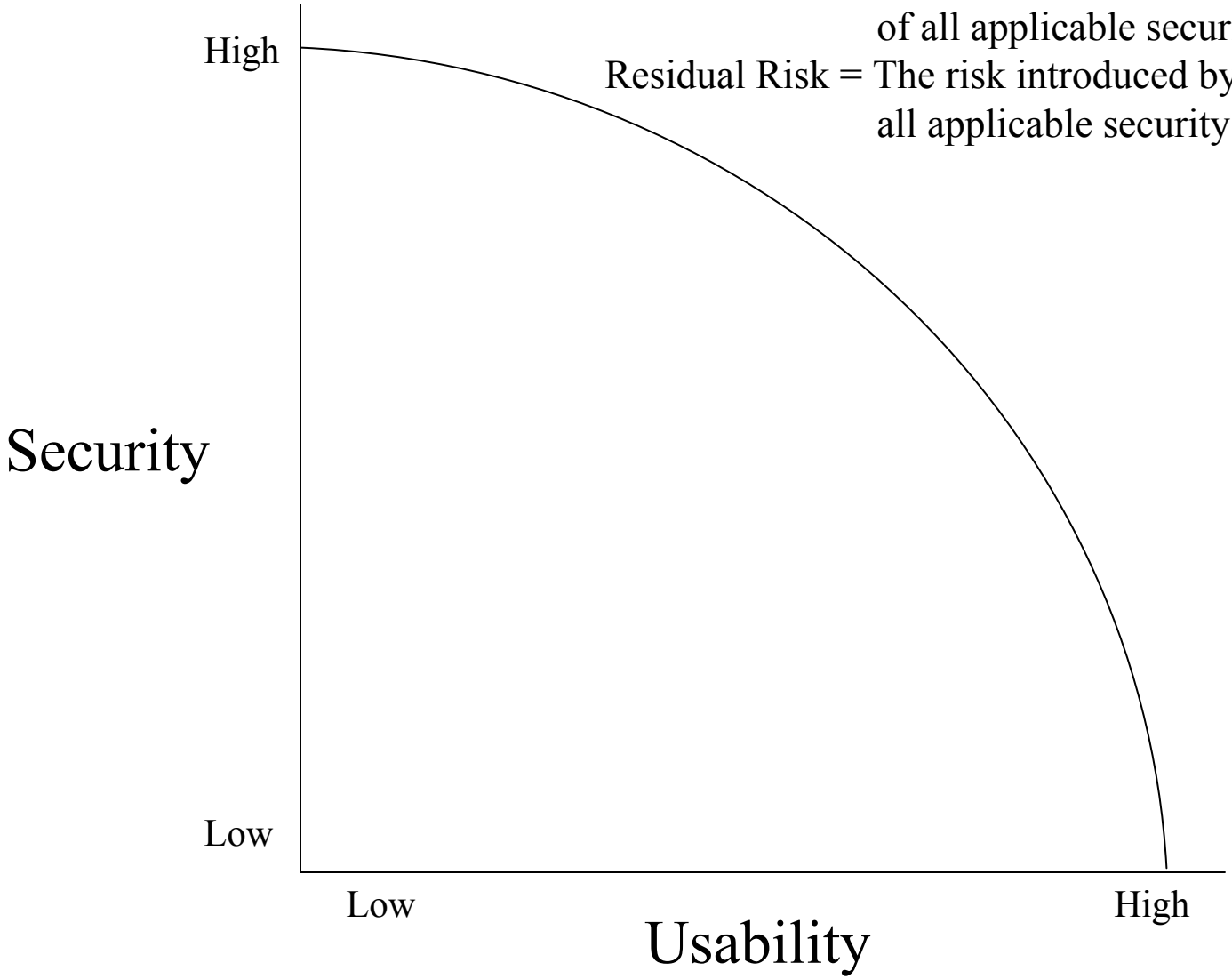
- Because execution is relatively expensive and difficult, the DITSCAP methodology is generally only applied to DoD systems that operate in a *production* mode.
- Within most DoD areas, no resources are generally applied in support of DITSCAP efforts without the prior and explicit approval of senior leadership.
- In special circumstances, an Interim Approval To Operate (IATO) may be pursued, but only as part of a stepping stone migration strategy towards an imminent or near-term DITSCAP effort.
- An IATO is *not* an alternative to a DITSCAP-compliant C&A effort and should only be considered in extraordinary or extenuating circumstances.

TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

The Risk Tradeoff between Security and Usability

Zero Risk = The elimination of risk through satisfaction of all applicable security requirements

Residual Risk = The risk introduced by not fully satisfying all applicable security requirements



TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

The Certification Sub-process in DITSCAP

- Certification is a DITSCAP sub-process that logically *precedes* Accreditation.
- Certification is the responsibility of the Certification Authority (CA).
- The purpose of Certification is to 1) determine the security requirements applicable to a given system, and 2) measure the extent to which the system satisfies its applicable security requirements and introduces *residual risk*.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

The Accreditation Sub-process in DITSCAP

- Accreditation is a DITSCAP sub-process that logically *follows* Certification.
- Accreditation is the responsibility of the Designated Approving Authority (DAA).
- The purpose of Accreditation is to have a clearly identified official – the DAA -- formally accept operational responsibility for running the system within a production mode based on its established *residual risk.*

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Major DITSCAP Parties

- Certification Authority (CA).
- CA support team.
- Designated Approving Authority (DAA).
- Project Contractor.
- Project Officer.
- Project User Representative.
- Project/Program Information Assurance Officer (IAO).
- Project/Program Information Assurance Manager (IAM).

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Major Process Attributes of DITSCAP

- Relies on process flows that reflect extensive checks and balances.
- Provides for *generation* of all required materials within three discrete implementation phases (Definition, Verification, and Validation) and *maintenance* of all required materials within a fourth phase (Post Accreditation).
- Emphasizes *consensus*, *collaboration*, and *coordination* between different parties, each of whom have different vantage points and clearly defined individual responsibilities.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Examples of Collaboration, Consensus, and Coordination in DITSCAP Activities

- Security testing (Project Contractor versus CA support team).
- Identification and remediation of security vulnerabilities (CA support team versus Project Contractor and Project IAO).
- Security documentation (Project Contractor versus CA support team).
- Certification (CA versus CA support team).
- Accreditation (DAA versus CA).

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

System Security Authorization Agreement (SSAA)

- The SSAA is a system-specific document mandated by the DITSCAP methodology.
- The purpose of the SSAA is to (a) record the outputs and products of all individual DITSCAP-related activities, and (b) serve as a compendium of all security data acquired during the execution of supporting DITSCAP activities.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

SSAA Content

- The SSAA for a given system must contain *minimum* content prescribed by DoD Instruction 5200.40.
- The SSAA for a given system should include all relevant:
  - Security documentation.
  - Security test data.
  - Vulnerability assessment data.
  - Certification paperwork from the CA.
  - Accreditation paperwork from the DAA.
- The SSAA is intended to be a "living document" which is updated in a timely fashion when the system changes.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

SSAA Organization

- The SSAA for a given system must be structured consistent with the guidance provided by DoD Instruction 5200.40 and DoD 8510.1-M.
- In recognition that "one size does not fit all," both DoD Instruction 5200.40 and DoD 8510.1-M permit the SSAA format to be *extensible* and *customizable*.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Basic Layout of the SSAA

- Core SSAA (chapters 1 through 6). This portion of the SSAA contains *summary-level* security information on the system and represents the "driver" of the overall document.
- SSAA Appendices. This portion of the SSAA contains *detail-level* security information on the system and is largely based on a collection of individual standalone documents, each of which is placed in an individual SSSA appendix. It represents the preponderant bulk of the overall SSAA content.

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Organizational Scheme of Core SSAA Per DoD 8510.1-M

Chapter	Name/Title
1	Mission Description and System Identification
2	Environment Description
3	System Architectural Description
4	System Security Requirements
5	Organizations and Resources
6	DITSCAP Plan

TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

Organizational Scheme of SSAA Appendices Per DoD 8510.1-M

Appendix	Title/Name
A	Acronyms
B	Definitions
C	References
D	System Concept of Operations
E	Information System Security Policy
F	Security Requirements and/or Requirements Traceability Matrix (RTM)
G	Certification Test and Evaluation Plan and Procedures
H	Security Test and Evaluation Plan and Procedures
I	Applicable System Development Artifacts or System Documentation
I-1	Security Features User's Guide (SFUG)
I-2	Trusted Facility Manual (TFM)
I-3	Security Design Document (SDD)
I-4	Configuration Management Plan (CMP)
I-5	Installation Guides (*optional*)
J	System Rules of Behavior
K	Incident Response Plan
L	Contingency Plans
M	Personnel Controls and Technical Security Controls
N	Memorandum of Agreements – System Interconnect Agreements
O	Security Education, Training, and Awareness Plan
P	Test & Evaluation Report(s)
Q	Residual Risk Assessment Results
R	Certification and Accreditation Statement

TEAM INC.
TECHNOLOGY, AUTOMATION & MANAGEMENT, INC.

In terms of its long-term intent, has DITSCAP been successful?

- DITSCAP today reflects a mixed record in terms of fulfilling its long-term intent and potential.
- DITSCAP has been a *success* in the sense that it represents a mandatory baseline process for each and every production DoD system.
- DITSCAP has been a *failure* in the sense that a) it has not kept pace with the DoD sector's increased emphasis on security within the Post-911 world, and b) it does not as of today represent a complete A to Z solution that addresses all Service-specific security considerations. Examples of problem areas include the current Ports, Protocols, and Services initiatives as well as the proprietary Army and Air Force CON processes.
- Within the next few years, DITSCAP is slated to be replaced as the mandated DoD C&A methodology by a relatively more *net-centric* approach called DoD Information Assurance Certification and Accreditation Process (DIACAP).