

“Reciprocity”



Directorate for Information Management & CIO



Steve Fager, Acting DIA CIAO
SEP 2009

This briefing is classified
UNCLASSIFIED

“BLUF”



Directorate for Information Management & CIO

- The DoD CIO and ODNI, C&A Reciprocity methodology, developed under the C&A Revitalization Initiative, will enable Department of Defense and Intelligence Community (IC) Agencies to accept each others security certifications without having to conduct further security testing. The concept of C&A Reciprocity is in the best interest of the DoD and IC in order to maximize reuse of security certification testing.

The Vision



Directorate for Information Management & CIO

- Reciprocity Plan establishes a streamlined, common and shared process to address multiple disparate and inconsistently applied Information Technology (IT) C&A processes causing unnecessary delay in systems delivery, technology adoption and information sharing.
- The ODNI CIO and DoD CIO believe this approach will allow certified connections within and between agencies and departments to be made in less time and with minimal effort.



The Goal

Directorate for Information Management & CIO



The goal is to deploy and certify technology in days and weeks versus months and years.

Talking Points



Directorate for Information Management & CIO

- C&A Reciprocity for systems is the acceptance of another organization's certification that the protection controls are sufficiently applied to the system without the need to conduct supplementary validation or verification tests.
- C&A Reciprocity also allows the interconnecting of separate systems or networks with different certifying agencies without further certification testing of either of those entities, while each respective organization maintains their accreditation authority.

Talking Points



Directorate for Information Management & CIO

- **Certification & Accreditation**
 - Implement a C&A process that formally identifies and assesses threats, vulnerabilities and consequences to establish a managed accreditation decision based on a defined level of risk
 - Create and populate web-based C&A database to identify and track C&A activities
 - Ensure management of an Accreditation Process
- **Compliance Verification (e.g., Metrics & Reporting)**
 - Implement a cohesive process to ensure the right IA information is being collected, analyzed, and reported to support Risk management decisions
 - Developing an IA Metric Implementation Plan and Taxonomy
 - Develop a plan for continuous monitoring
- **IA Career Management & Training (DoD 8570.1)**
 - Create an educated and trained core of IA professionals
 - Institutionalize the IA workforce at all levels across the Enterprise

Talking Points (cont)



Directorate for Information Management & CIO

- Reciprocity is based upon adopting a common C&A Approach
 - Dependant on consistent implementation of a standard set of security controls
 - Dependant upon one C&A policy
 - Dependant upon final implementation details; Process execution
 - Dependant upon DAA acceptance of other DAA accrediting decisions
 - C&A decision-making is organization centric; wide interpretation of 'acceptable operating risk'

Where are we?



Directorate for Information Management & CIO

- All organizations consistently apply standardized security controls across national security systems
 - Use common controls contained in NIST SP 800-53 as “baseline”
- IC and DoD shall develop guidance for “shared” controls not addressed by NIST SP 800-53 (CNSS 1253)
 - Include “shared” controls in updated IC and DoD guidance
 - IC and DoD security control documents will reference NIST SP 800-53 “baseline” controls
- Long-term goal is to document all Federal guidance in one document, preferably NIST SP 800-53

Next Step:

- Follow-on effort to create guidance which identifies IC/DoD gaps with NIST and create “shared” IC/DoD security controls for national security systems

Where are we?



Directorate for Information Management & CIO

SP 800-53 (REV 3)	Security Controls	Highest NIST priority. Released for public review 2 June. Final publication target 31 Jul 09
SP 800-37	Applying the Risk Management Framework to Federal Information Systems	Second Highest NIST priority. Delayed approx 1 month. Final publication target 30 Sep 09
SP 800-39	Managing Risk from Information Systems: An Organizational Perspective	Managing Risks to Organizations. Target approval date Oct 09
SP 800-30	Risk Management Guide	Will focus on risk assessment concepts within RMF. Target approval date Dec 09
SP 800-53A	Security Assessments: Tools for Measuring the Effectiveness of Security Controls	Assessment criteria for 800-53 controls. Target approval date spring 2010

Where are we?



Directorate for Information Management & CIO

Agreement Signed by Mr John Grimes, Department of Defense Chief Information Officer and Mr Dale Meyerrose the Intelligence Community Chief Information Officer, 22 August 2008.

The Department of Defense and the Intelligence Community are adopting common guidelines to streamline and build reciprocity into the certification and accreditation process . These common certification and accreditation efforts will conserve manpower and resources, build efficiencies, and eliminate wasted efforts reformatting packages between the Department of Defense and Intelligence Community .

Where are we?



Directorate for Information Management & CIO

- DoD issued “DoD Information System Certification and Accreditation Reciprocity” Memorandum, 23 July 2009
 - Defines reciprocity as: “mutual agreement among participating enterprises to accept each others security assessments in order to reuse IS resources and/or accept each other’s assessed security posture in order to share information”
 - C&A Supporting Security Terms and Conditions IAW DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) for Enterprise IS

Where are we?



Directorate for Information Management & CIO

- Defense IA Security Accreditation Working Group (DSAWG) will conduct enterprise security reviews
- DISN/GIG Flag Panel assess Information Enterprise risk, authorize information exchanges and enterprise connections IAW DoDI 8510.01
- DoD issuance/guides
 - DoD 8500.1/2 **NIST SP 800-53**
 - DoD 8510.01 **NIST SP 800-37, NIST SP 800-53A**
- Intelligence Community will use the NIST and CNSS documents as published.

Where are we?



Directorate for Information Management & CIO

- The Information Security and Risk Management Committee (ISRMC) assess Information Enterprise risk, authorize information exchanges and enterprise connections for the IC
- Most IC agencies continue to use DCID 6/3 Manual processes/documentation; contingent upon final approval of all NIST/CNSS guidance. Transition guidance in ICIA-2008-126

Are We There?



Directorate for Information Management & CIO

- Transformation Goals:
 - Define a common set of trust (impact) levels
 - **SP 800-53**
 - Adopt reciprocity
 - **Working**
 - Define, document, and adopt common security controls
 - **SP 800-53 & CNSSI 1253**
 - Adopt a common lexicon
 - **CNSS 4009**
 - Institute a senior risk executive function
 - **DISN/GIG Flag Panel for DoD**
 - **ISRMC for IC**

Are We There?



Directorate for Information Management & CIO

- Incorporate Information Assurance (IA) into Enterprise Architectures
 - **Working**
- Enable a common process
 - **NIST SP 800-37**
 - **ICD 503**
 - **DoD 8510.01**

?



Challenges to “Reciprocity”

Directorate for Information Management & CIO

- Acceptance!!!!
- Trust; i.e. Trust Agency Certifiers. Certifications by any certifying organization must be accepted for baseline security controls
- Tailoring of security controls will be an issue for all; but should be the key to recertification efforts; i.e. test the deltas
- Documentation differences between DoD and IC may be challenging; DIACAP vs ????.
- No common repository for C&A Doc's
- Collaboration is everything!!



Directorate for Information Management & CIO

Trust enables Reciprocity



Directorate for Information Management & CIO

DISCUSSION

QUESTIONS?

VIEWS