Overview of the DoD Information Assurance Certification and Accreditation Process - DIACAP

DARPA SBIR Phase I Workshop 2

Gleason Snashall
SPAWAR System Center – Pacific
CISSP/ISSEP, FQNCA, C&A TAE, PMS 501 IAM

Overview Questions

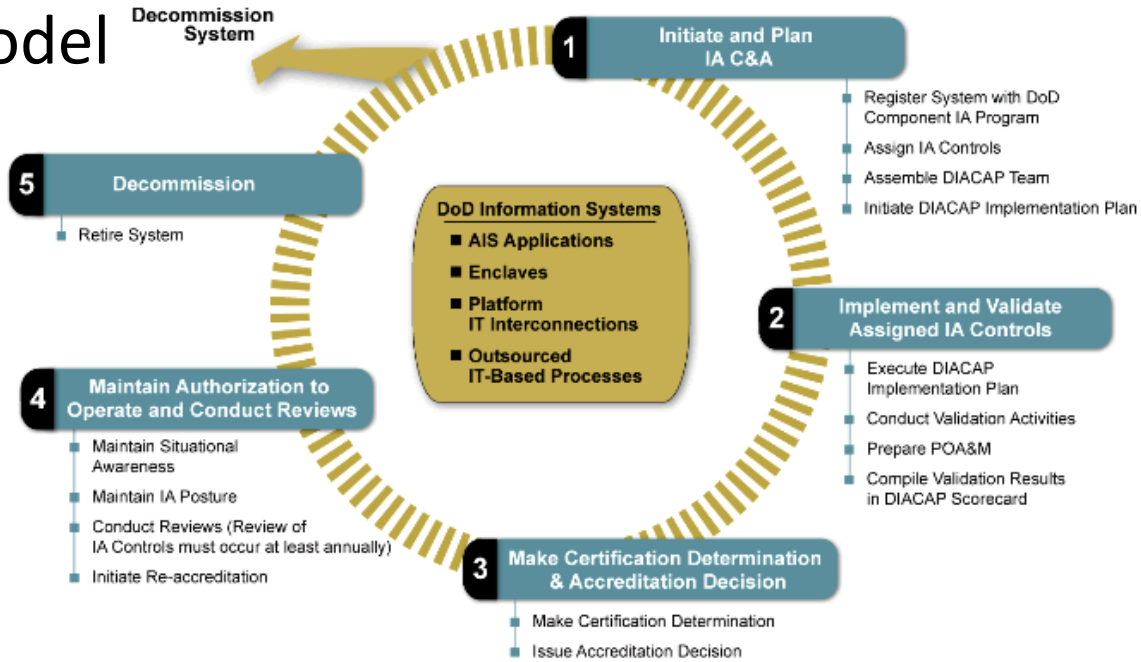
- What is DIACAP?
  - What requires DIACAP certification and accreditation?
  - What does the certification and accreditation process entail?
  - What is the timeline for going through the certification and accreditation process?
  - How can I best prepare for going through the certification and accreditation process?
- Other issues
  - Why is it important to receive certification and accreditation?
  - Who is responsible for the certification and accreditation process?
  - What does a company do if they don't receive certification and accreditation?
- Resources for companies to find more information

What Is DIACAP?

- Department of Defense (DoD)
  - Requirements will be tailored for DoD mission
  - Primary requirement set is based on DoDI 8500.2
  - Other requirements as threat evolves
- Information Assurance (IA)
  - Confidentiality
  - Integrity
  - Availability
- Certification and Accreditation (C&A)
  - Verify and validate that security requirements are met (certification)
  - Provide a statement of risk acceptability for operation and connection (accreditation)
- An IA Process

An IA Process

- It is a development model
  - Compare it to the classical waterfall development model
    - Requirements
    - Design
    - Implementation
    - Verification
    - Maintenance
    - Obsolescence



- Intended to be implemented during complete development cycle
  - Best preparation is to include IA from project inception
  - The certification and accreditation process lasts for the entire life cycle

Why Is C&A Important?

- SP800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

- **Risk**
  - Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
  - *"…Through the process of risk management, leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations…"* - THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS, OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

- **Likelihood of occurrence**
  - Vulnerability [CNSSI 4009] Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
  - Threat [CNSSI 4009, Adapted] Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

- **Impact**
  - High-Impact System [FIPS 200] An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
  - Moderate-Impact System [FIPS 200] An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.
  - Low-Impact System [FIPS 200] An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Other Issues

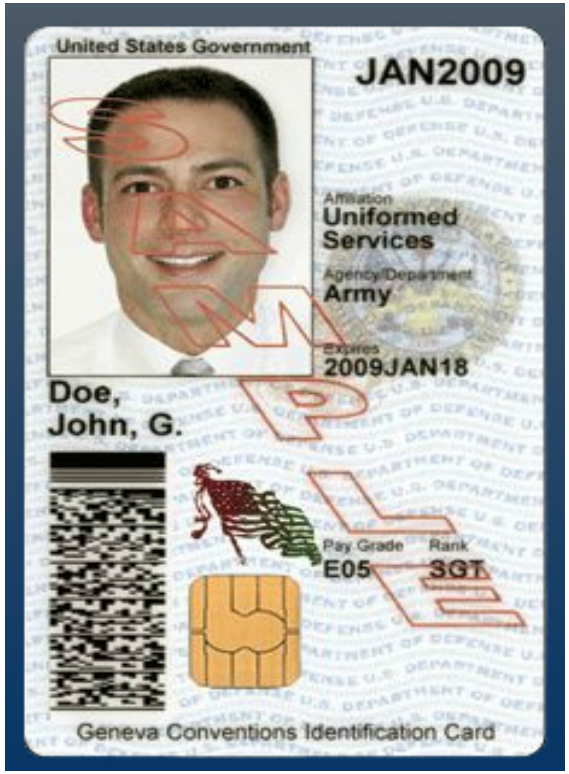
- How can companies best prepare to go through the process?
  - Commitment to IA
    - IA training
    - Program line item with IA from program inception to obsolescence
  - Knowledge of lines of authority
    - Who reviews the submitted documents
    - Who approves the request for an Authorization To Operate (ATO)
  - Configuration management (CM)
    - Configuration Control Board (CCB) charter / CM Plan (CMP)
    - CCB has IA manager as member
    - Commitment to CM
- What are some of the reasons for not receiving an ATO?
  - Inadequate definition of the accreditation boundary
  - Failure to perform all relevant tests
  - Failure to trace all results from IA requirement to risk assessment
  - Risk assessed as too high by DAA (e.g. end of life software, IA Vulnerability Alerts (IAVA) not patched, …)

Other Issues (Cont'd)

- Why is it important to receive certification and accreditation?
  - C&A provides the basis for risk management decisions
  - It is not a single event; recertification is annual
  - Certification and recertification are initiated by the program manager
- Who is responsible for the certification and accreditation process?
  - Each service and DISA have a Designated Approving Authority who is responsible for reviewing C&A submissions and approving operation of the system
- What does a company do if they don't receive certification and accreditation?
  - There is generally a process for resubmission of application for an Approval To Operate (ATO) – usually involves submission of a Plan of Action and Milestones (POA&M) for corrective measures
  - For certain activities, an Interim Approval To Test (IATT) may be issued to facilitate testing or experimentation over an extremely short time

Common Access Card (CAC)

- It is difficult or impossible to navigate through the necessary information and submission channels without a CAC
- Most sites on the useful resources page require a CAC login



Useful Resources

- NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- DIACAP specification https://diacap.iaportal.navy.mil/ks/SiteResources/Reference%20Library/Base/General%20Documents/851001p.pdf
- Testing
  - SCAP Web site: http://scap.nist.gov
  - DISA Retina / SCAP brief: https://powhatan.iiie.disa.mil/tools/sccvi/updates/unclassified_eEyeRetinaSCAP_Brief_20101004.pdf
  - DISA Retina documentation (contains sub-;links to User Guide/Installation Guide/Common Configuration/Checklist/etc.) https://powhatan.iiie.disa.mil/tools/sccvi/documentation/
- DISA Information Assurance Web Page http://www.disa.mil/services/ia.html
- Knowledge base https://diacap.iaportal.navy.mil/KS/Pages/default.aspx
- Air Force:
  - https://www.my.af.mil (Login/registration required)
  - https://afkm.wpafb.af.mil/ [Knowledge-Now Portal similar to NKO. (CAC & Login/registration required)]
- Army:
  - www.army.mil/ako (All department publications including distro-restricted items)
  - www.apd.army.mil (Army publishing directorate for publications & forms)
- Navy
  - https://www.portal.navy.mil/netwarcom/navycanda/default.aspx