Cybersecurity Webinar Series

Industry's Role in the C&A Process

Overview

- Define the C&A Process
- Consider each step in the C&A Process
- Discuss the OBMS actions that relate to the submission process
- Provide resource links for future reference

NISP C&A Process

- Re-evaluation
- Self-Assessments
- Facility Reviews
- Re-accreditation
- Re-evaluation
- Self-Assessments
- Facility Reviews

Initiation and Planning
- Determine Security Requirements
- Develop system security plan

System Development
- Build, Configure, Test, Certify
- Submit Security Plan (SSP)

Review and Certification
- Plan Review or Onsite Validation
- Recommendation Issues DATO, IATO, or ATO

Disestablish when no longer needed or Contract Expiration
- Disestablishment

Continuous Review
- Re-evaluation
- Self-Assessments
- Facility Reviews
Where we’ve been and where we’re going

Old Process

New Process

The C&A Process helps protect classified information systems against:

- Unauthorized access to or modification of information
- Denial of service to authorized users

Industry’s Role in the C&A Process helps to protect, detect, characterize, counter, and mitigate unauthorized activities and vulnerabilities.

Polling Question 1

- How many steps are there in the NISP C&A Process?
  - 3
  - 4
  - 5
  - 6
### Resource Links

These are helpful resource links related to the NISP C&A Process

- NISPOM - [http://www.dss.mil/isp/odaa/nispom06.html](http://www.dss.mil/isp/odaa/nispom06.html)
- OBMS Training - [http://www.cdse.edu/catalog/elearning/CS120.html](http://www.cdse.edu/catalog/elearning/CS120.html)

### NISPOM Chapter 8

- Prescribes safeguards necessary to prevent unauthorized disclosure of classified information.
- Identifies security requirements for contractor Information Systems (IS) that process classified information.
- Assigns responsibility to DSS for establishing a line of authority for training, oversight, program review, certification and accreditation of contractor’s IS.

### ODAA Process Manual

- Designed to provide a resource for DSS staff, ISSMs, and ISSOs.
- Explains process standards, interpretation standards, technical configuration standards, and system security plan standard templates.
NISP C&A Process – Step 1

- Initiation and Planning
  - Receive DD 254
  - Determine Security Requirements
  - Develop system security plan

- System Development

- Continuous Review

- Disestablishment

- Accreditation Decision

- Review and Certification


NISP C&A Process – Step 2

- Initiation and Planning

- Disestablishment

- System Development

- Build, Configure, Test, Certify

- Submit Security Plan (SSP)

- Continuous Review

- Accreditation Decision

- Review and Certification


OBMS - Home Page

- Office of the Designated Approving Authority (ODAA) Business Management System

- OBMS Home Page - Contractor Submitter

- Notifications

- Task

- Subject

- [1234567890]
OBMS - Starting the Process

OBMS – General Plan Information

OBMS – System Information
Polling Question 2

Which button must you press after entering all System Information before you can access other tabs?

- Validate
- Save
- Exit

OBMS – Assets Tab

OBMS – Add System
Polling Question 3

- What's the correct way to save a template when working online in OBMS?
  - Use the Adobe Acrobat Save command
  - Use the Save Form button inside the template
Chat Question

- What do you think happens if submit the package and you haven’t provided an electronic signature for the Information System Profile?

Type your responses in the chat window and let’s see what the consensus is.

OBMS – Other Options

Industry’s Role in the C&A Process can help to protect, detect, characterize, counter, and mitigate unauthorized activities and vulnerabilities, and helps address areas for improvement in securing the classified information technology infrastructure.
Questions

Cybersecurity Training Products and POC

Past Webinars
- [http://www.cdse.edu/catalog/webinars/webinar-archives.html](http://www.cdse.edu/catalog/webinars/webinar-archives.html)

All Other Training
- [http://www.cdse.edu/catalog/cybersecurity.html](http://www.cdse.edu/catalog/cybersecurity.html)

Christopher Cox
Phone: (410) 689-1398
Email: cybersecurity.training@dss.mil