U.S. Army Research, Development and Engineering Command

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Use of Security Overlays or Control Sets in Addressing Control Deviations for Mortar Systems

27 April 2016

Mr. Daniel F. Campbell – U.S. Army ARDEC, Picatinny Arsenal

DistributionStatement A. Approved for public release: distribution unlimited.

Discussion

- **Background.**
- **Issues.**
- **What is an Overlay and Control Set?**
- **How Overlays and Control Sets can benefit Mortar Systems.**

DistributionStatement A. Approved for public release: distribution unlimited.

Background

In March of 2014, the Department of Defense (DoD) reissued Department of Defense Instruction (DoDI) 8510.01 and renamed it to "Risk Management Framework (RMF) for DoD Information Technology (IT)." This change replaced DoD Information Assurance Certification and Accreditation Process (DIACAP) with RMF.

This change brought with it several changes to Certification and Accreditations.

Changes the way DoD addresses security.

Malcolm Baldrige National Quality Award 2007 Award Recipient
DistributionStatement A. Approved for public release: distribution unlimited.

First noticeable change:

- Control changes
  - Family of Controls:
    - DIACAP - **9** -> RMF - **18**
  - Controls:
    - DIACAP* - **110** -> RMF** - **512**
  - Validation Procedures:
    - DIACAP* - **171** -> RMF** - **1936**

*DIACAP Numbers Based on MACII/Classified System.
**RMF Numbers based on CIA (Medium/High/High) with Classified Overlay.

Malcolm Baldrige National Quality Award 2007 Award Recipient
DistributionStatement A. Approved for public release: distribution unlimited.

Background

Other changes:

- Risk based to be more proactive than reactive.
- Continuous monitoring and reporting focused to be able to determine actual risk as the systems are used and to address ever-changing threats.
- Extremely inclusive to better determine actual risk.

DistributionStatement A. Approved for public release: distribution unlimited.

Issues

RMF is applicable to all DoD IT that receive, process, store, display, or transmit DoD information.

DoD IT will be required to be registered in the Enterprise Mission Assurance Support Service as "Assess and Authorize" or "Assess Only."

Assess Only will be replacing Certificate of Networthiness.

DistributionStatement A. Approved for public release: distribution unlimited.

Issues

Currently there are several assumptions made about a system being assessed.

- Systems are on a network if they communicate.
- Systems can fulfill all mandates that have been issued.
- Systems are general use that have been modified to meet mission need.

Deviations from these assumptions are addressed on a case by case basis during the assessment process.

DistributionStatement A. Approved for public release: distribution unlimited.

Issues

Significant upfront time and money for initial registration and assessment of new IT.

- Currently time needed is estimated 6-12 months of effort for initial RMF Authorization.
  - Most of the time will be on the comprehensive self assessment.
- Mission specific tactical systems are unique and do not easily fit into common system types.
  - Additional time needed to address unique conditions
- There is a lack of personnel with experience in RMF assessments of deviating systems.

Malcolm Baldrige National Quality Award 2007 Award Recipient
DistributionStatement A. Approved for public release: distribution unlimited.

Issues

There is also a lack of lessons learned and information sharing of similar type systems.

- There are several meetings and groups the discuss specific controls or group of controls.
- No overall group to facilitate total system view that address common issues or information sharing.

DistributionStatement A. Approved for public release: distribution unlimited.

Overlays and Control Sets

The Committee on National Security Systems Instruction (CNSSI) 1253, states:

"An overlay is a specification of security controls and supporting guidance used to complement the security control baselines and parameter values in CNSSI No. 1253 and to complement the supplemental guidance in NIST SP 800-53."

DistributionStatement A. Approved for public release: distribution unlimited.

Overlays and Control Sets

Additionally,

“Overlays may be applied to reflect the needs of different information types (e.g., personally identifiable information [PII], financial, or highly sensitive types of intelligence); system functionality needs (e.g., stand-alone systems, cross domain solutions, or controlled interface systems); or environmental or operationally-driven needs (e.g., tactical, space-based, or test environment).”

DistributionStatement A. Approved for public release: distribution unlimited.

Overlays and Control Sets

Current Overlays:

- NSS Specific:
  - Cross Domain Solutions
  - Space Platform
  - Intelligence (FOUO)
  - Classified Information
  - Privacy
- Functional Mission Specific:
  - Nuclear Command and Control, Communications Systems Overlay

DistributionStatement A. Approved for public release: distribution unlimited.

Overlays and Control Sets

Control sets:

- Army Policy Record
  - Addresses controls that are covered by Army and/or DoD policies.
  - Covers approximately 324 assessment procedures.

DistributionStatement A. Approved for public release: distribution unlimited.

Overlays and Control Sets

The process for overlay development is in the “DoD Risk Management Framework Overlay Development Guidance.”

This guidance can be found on the RMF Knowledge Service.

DistributionStatement A. Approved for public release: distribution unlimited.

Benefits

Overlays and/or custom control sets could be used to standardized system security requirements and/or compliancy across multiple systems of similar type.

- The overlay would be able to address specific controls that may not be possible to implement.
- The overlay could define and possibly address the common controls with in mission specific group under one artifact.
- Allows for better visibility of areas that should have more focus of resources.

DistributionStatement A. Approved for public release: distribution unlimited.

Benefits

This can provide common answers to controls.

- These may have already been reviewed and accepted by the Security Control Assessors (SCA). If this is the case, it should reduce the time needed for some of the reviews.

- If the answers are common, additional resources should not be needed for initial assessments and reviews.

DistributionStatement A. Approved for public release: distribution unlimited.

Example

Configuration Management documentation.

- Organizational Standard Procedures
- Configuration Management Plan
- Project Plan
- Configuration/Data Management Audit

Able to generate an initial Control Set of:

- Control Family – CM/SA/SI
- Controls – 41
- Validation Procedures – 131

DistributionStatement A. Approved for public release: distribution unlimited.

Example

Use of Control Set.

- Matrix for tracing CM Information Assurance requirements and compliance.
- Possible inclusion of control information in to CM templates to assist future projects.
- Assist in ensuring Information Assurance information within the documents do not get tailored out.

DistributionStatement A. Approved for public release: distribution unlimited.

Summary

- **Changes to Certification and Accreditation Process.**
- **Current issue Fire Control faces.**
- **What are overlays and control sets, and how they work.**
- **Benefits of using overlays and control sets.**

DistributionStatement A. Approved for public release: distribution unlimited.

Questions

Malcolm Baldrige National Quality Award 2007 Award Recipient

DistributionStatement A. Approved for public release: distribution unlimited.