
# Appraising Classified Programs

Bob Moore
Senior Principal Process Engineer
www.biztransform.net

Business Transformation Institute

# Could Being On A CMMI Appraisal Team Earn You Federal Jail Time?

- Yes!
- Disclosure of some appraisal results may result in you being fined or imprisoned under United States Code Title 18, Part 1, Chapter 37, Section 798.
- Now that I've got your attention . . . how exactly could that happen?

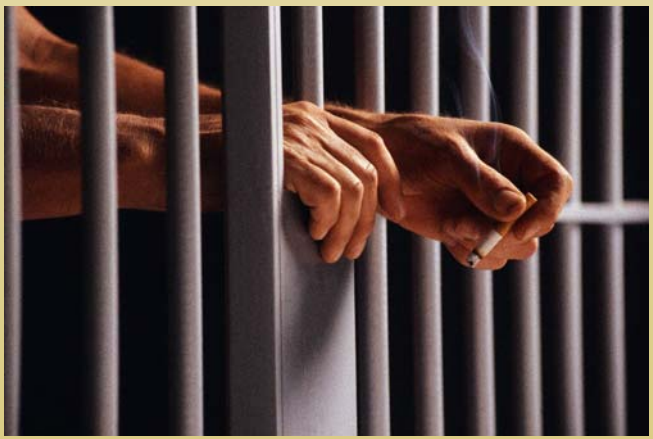

# CMMI Appraisals On Classified Programs

- Many organizations using the CMMI have programs classified by the US Department of Defense.
- We'll label a program meeting one or more of the conditions below as a "classified program":
  - Artifacts produced by the program are classified.
  - The existence of the program is classified.
  - The identities of people working on the program are classified.
  - The association of the program with a particular facility or organization is classified.

Business Transformation Institute

# What About The Federal Jail Part?

- Appraisal disclosure statements (ADS), appraisal plans, appraisal results, etc. from classified programs could contain classified data.
- By the way, unauthorized release of classified information damages the national security of the United States . . . and may earn you jail time.



# Shouldn't We Just Avoid Appraising Classified Programs?

- YES--if appraising a program will inevitably lead to unauthorized disclosure of classified information!
- However, conducting a legitimate appraisal of an organization may mean that some of the appraised programs will be classified.
  - The SCAMPI Method Description Document (MDD) version 1.2, section 1.1.3, states:

    *Sample projects and support groups selected to form the organizational scope (i.e., the combination of focus and non-focus projects and support functions) must represent all critical factors identified for the organizational unit to which the results will be attributed.*
  - Program classification should be regarded as a "critical factor" unless shown to be otherwise.

# Is Classified Versus Unclassified Program A Critical Factor? (1)

- The SCAMPI MDD v. 1.2 obliquely defines critical factors in the following sentence:
  - *Critical factors that influence implementation of practices in projects and functions within the organizational unit must also be understood and identified.*
- Parsing this sentence, we understand that the "critical factors" in which we are interested are those aspects of the organization that influence how processes are implemented in the various "projects and functions" in an organization.

# Is Classified Versus Unclassified Program A Critical Factor? (2)

- Program classification should be considered one of these factors because:
  - The personnel who work directly on classified and unclassified programs may be mutually exclusive within an organization.
  - The process support personnel who support classified and unclassified programs may be mutually exclusive.
  - There is less visibility into and sharing of results (GPs 2.8, 2.10, 3.2) on classified programs.
- All of these lead to classified and unclassified programs having different process implementations.


# Objective: Plan and Conduct An Appraisal Of A Classified Program

- Just because some aspect of a program is classified does *not* mean that:
  - The program cannot be appraised or
  - The appraisal results cannot be published in the Software Engineering Institute's (SEI) Published Appraisal Results (PARS) database.
- This presentation suggests techniques for appraising classified programs and possibly publishing results in PARS without having unauthorized disclosure of classified information.
- Note: the SEI Appraisal System (SAS) has a mechanism for indicating that programs are sensitive on a program-by-program basis.

# Classified Program Appraisal Scenarios

- This presentation addresses appraising classified programs using the following scenarios.
- The techniques used to address each scenario may be combined when the actual appraisal situation represents multiple scenarios.
  - The presentation cannot cover every nuance!
- The scenarios cover the following circumstances:
  - Programs with classified artifacts.
  - Classified (black) programs.
  - Program personnel with cover identities.
  - Programs or customers that cannot be associated with a particular location or organization.


# Scenario 1: Classified Appraisal Artifacts

- Our story:
  - The US Navy is tasked with intercepting and destroying missiles launched from the People's Republic of China during any outbreak of hostilities with the Republic of China (Taiwan).
  - To support this mission, the US Navy is acquiring the **S**traits **o**f **F**ormosa **M**issile **O**cclusion **R**adar **S**ystem (SOFMORS) from MegaBucks Missiles and Space, an aspiring CMMI Maturity Level 5 company.
  - The existence of SOFMORS is well known—there have even been debates in the US Congress about the pork barrel politics of why the Navy is spending billions on second year college students!
  - Unfortunately the requirements, system architecture and design, test cases, validation scenarios, etc. are classified.
  - MegaBucks has come to SEI High-Maturity Appraisal Consultants, LLC (SHAC) to plan a Maturity Level 5 appraisal for them.


# Appraising SOFMORS

- SOFMORS' classified artifacts are in the CMMI's engineering process areas: Technical Solution, Product Integration, Verification, Validation, Requirements Management, and Requirements Development.
- The existence of classified artifacts is a challenge. SOFMORS staff comprises almost half of MegaBuck's personnel—this program is definitely in scope for the appraisal!
- How can SHAC handle appraising SOFMORS?


# Technique 1: Unclassified Artifacts

- Even on programs with classified data, many key artifacts will *not* be classified.
  - This "technique" is straightforward—appraise a classified program without ever looking at classified information!
- SOFMORS may be able to identify direct and indirect artifacts for the appraisal without referencing the classified artifacts.
- Unfortunately, this will often not be the case—especially when the classified data comes from the engineering process areas.
  - Along with budget, program size, and program milestone information, a program's technical data is often the most classified aspect of the program.
- To apply technique #1, MegaBucks needs an artifact collector who is:
  - Cleared to look at SOFMORS' data and
  - Sufficiently knowledgeable about the CMMI and appraisals to be able to identify good artifacts.


# Technique 2: Redact the Artifacts

- Redaction means "to edit or revise something in preparation of publication".
  - Redacting classified information means removing the classified content. The remaining information is unclassified.
- The classified aspect of an artifact may *not* be of interest with respect to a CMMI appraisal.
  - For example, in a system requirements document, the actual value of a technical performance measures (TPMs) (e.g., designed antenna gain) may be classified—but the TPM itself may not be.
  - The appraisal team does not care about the actual value of the TPM, only the existence and use of the TPM.
- Unfortunately, redacting documents is expensive and time consuming for the organization and program.
- To apply technique #2, MegaBucks needs:
  - An artifact collector who is cleared for the program, knowledgeable about appraisal artifacts, and who can redact the artifacts.
  - SOFMORS security personnel to approve the redacted artifacts.

# Technique 3: Cleared Appraisers

- This technique is obvious—but important.
- If the artifacts are classified, then cleared appraisal team members will remove the challenge of classified artifacts!
  - Remember, authorization to look at classified data = eligibility + access + need-to-know.
  - Getting authorization for the appraisal team requires the cooperation of SOFMORS' customer!
    - Elicit the support of the appraisal sponsor and SOFMORS security.
- Not everyone on the appraisal team will need to be authorized for access:
  - At least one mini-team must be authorized.
  - Authorizing access for the lead appraiser is not required, but will help by increasing appraisal credibility and reducing appraisal planning costs.
- To apply technique #3, SOFMORS needs:
  - The US Navy to grant authorization to appraisal team members.
  - SOFMORS security personnel to approve the release of characterizations and findings to anyone not SOFMORS-cleared.

# Getting Program Security's Cooperation

- Program security will *not* want to help you!
  - Security personnel have plenty to do—supporting a CMMI appraisal is not on the list.
  - Security's primary responsibility is to protect classified data, not release artifacts.
    - The easiest, lowest-risk answer for many security officers for an activity that is not clearly mission related is "no".
- Help security to help you.

Business Transformation Institute

# Help Security to Help You! (1)

- Ask the appraisal sponsor to explain to security and the customer why the appraisal is important.
- Approach security six months to 12 months before the appraisal to explain:
  - How an appraisal works and
  - What will be done with the appraisal results.

# Help Security to Help You! (2)

- Include security in the appraisal planning process:
  - Selecting the appraisal team, particularly team members requiring access to classified artifacts.
    - Determining the conditions for access to the program.
    - Determining the eligibility status of team members.
    - Understanding how security processes visit requests:
      - Information required,
      - Proper communication channels, and
      - Time required.
  - Determining how much time security will need to review characterizations, findings, or redacted artifacts.
  - Determine key dates in the appraisal sequence when security will be needed.
  - Confirm review times and dates in writing!
  - Create an appraisal classification guide.

# The Appraisal Classification Guide

- Classified programs typically have a document that guides appropriate classification of program data.
  - The classification guide is developed under the customer's direction.
- Developing an appraisal classification guide with security's approval will help manage the expectations and time required for characterization and findings review.
  - The purpose of the security guide is to anticipate security classification review challenges and establish a documented agreement in advance to avoid these challenges.
  - The primary user of the guide will be the mini-teams and program security, since the mini-teams processes classified artifacts into unclassified findings and characterizations that are reviewed by security.

Business Transformation Institute

# Appraisal Classification Guide Content (1)

- The typical communications channel between the mini-team and the rest of the appraisal team is the appraisal workbook.
- The SEI's standard appraisal team workbook contains the following fields that are usually filled in at the mini-team level:

| Goal | Practice | Project | Type | Inst Char | Weakness (Description of gap in implementation) Strengths are Optional | Information Needed |
|---|---|---|---|---|---|---|

- The "Goal", "Practice", and "Project" fields are pre-determined and do not needed to be reviewed by security.

# Appraisal Classification Guide Content (2)

- "Type":
  - Consists of two fields:
    - The SCAMPI appraisal artifact type
    - Possibly a brief identifier of the actual artifact cited.
  - The SCAMPI artifact type is one of three known values (D, I, A) and does not need to be reviewed by security.
  - The description of the artifact being cited could contain classified data.
    - The actual titles of program artifacts are not typically of importance in an appraisal.
    - The key information in this field is the nature of the artifacts being reviewed.
  - The SEI's SCAMPI PIID examples contain unclassified key phrases that could be used to describe the artifacts observed.
    - Using these phrases in place of actual artifact names will ensure that this field contains unclassified data.

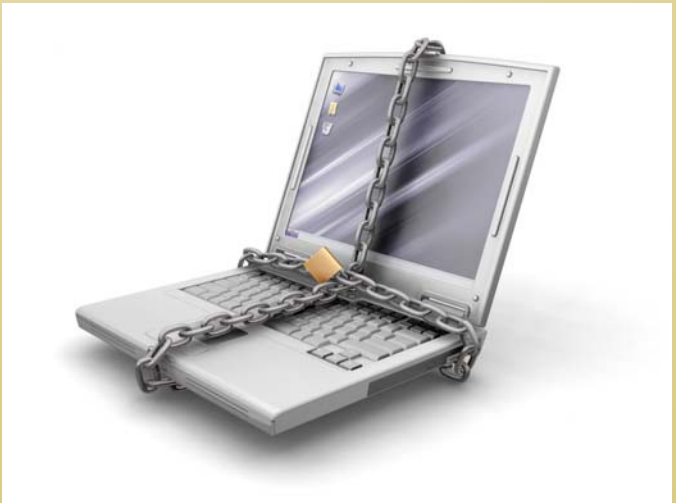
# Appraisal Classification Guide Content (3)

- "Inst Char":
  - Consists of one of five values (FI/LI/PI/NI/NY).
  - These values are not classified and do not need to be reviewed by security.
- "Instantiation-level Weakness (Description of gap in implementation) Strengths are Optional":
  - This field explains the weaknesses or strengths against the CMMI observed by the mini-team for the program.
  - Depending on the contents of the weakness or strength statement, this field could contain classified data.

Business Transformation Institute

# Appraisal Classification Guide Content (4)

- "Information Needed":
  - This field could contain classified data.
  - However, the field need not used by the full appraisal team but just by the mini-team.
  - Information in this column should be withheld from the full appraisal team, removing the need for security review.




# Scenario 2: Classified Programs

- Our story:
  - The National Security Agency (NSA) has been tasked by the Director of National Intelligence to develop a program to predict the actions of foreign leaders by monitoring their thoughts.
  - To support this mission, NSA is developing a program with cover name BABYLON. To support this program, NSA will issue a sole-source contract Psi Corp. Psi Corp has somehow intuited that NSA's sole-source justification will depend on Psi Corp maintaining a CMMI ML 2 on BABYLON.
  - The existence of the BABYLON program is classified.
  - Psi Corp is trying to figure out how to appraise BABYLON without telling anyone about it.

# Appraising BABYLON

- Unlike SOFMORS, everything about BABYLON is classified except for its cover name!
- Discussing any aspect of BABYLON will require that the appraisal team be granted access to the program.
- How can Psi Corp even contemplate having an appraisal on BABYLON?

# Revisiting Technique 3: Cleared Appraisers

- The "black" nature of BABYLON means that techniques 1 and 2 will not be applicable.
- Applying technique 3 may work. There are two possible approaches:
  - Use an appraisal team that is cleared to the level of BABYLON but that is not in the BABYLON compartment.
    - In this approach, techniques 1, 2, and 3 may work where the "unclassified" and redacted artifacts are really being moved from classification "X with a compartment" to just classification "X".
    - The appraisal team will not know anything about BABYLON, just that a program is providing artifacts.
  - Use an appraisal team that is cleared for the BABYLON compartment.
    - This is the best solution due to the sensitive nature of BABYLON.
    - This is unlikely—the personnel in the BABYLON compartment and the personnel able to appraise the program may be mutually exclusive.


# Appraisal Results for Classified Programs

- If Psi Corp manages to get BABYLON appraised, can the results be reported in the SEI Appraisal System (SAS)?
- Yes, with some precautions.
- SAS allows the Lead Appraiser to indicate that a program is “sensitive”.
- The details of a sensitive program as reported in SAS can be transformed to reflect reality without releasing classified information.
  - Example: For the description of the program, do not say “Intelligence collection through ESP” but instead “data survey and collection”.

Business Transformation Institute

# Scenario 3: Cover Identities

- Our story:
  - Personnel working on the FBI's DARK KNIGHT terrorism suppression system will need to install, configure, and test their system in nations around the world.
  - Since neither the FBI nor the nations receiving DARK KNIGHT want the personnel installing the system to be at risk once they return home, each person has been provided with a cover identity.
    - The cover identity provides each person with a passport and employment history not associated with who they really are. For example, DARK KNIGHT's chief engineer has a passport listing her identity as Selina Kyle.


# Appraising DARK KNIGHT

- The restrictions of scenarios 1 and 2 may also apply here.
  - We consider only the cover identity aspect.
- The key challenge in appraising DARK KNIGHT will be in concealing the identities of the people actually involved in association with the program.
- The most difficult aspects of this challenge are:
  - Conducting the affirmation collection sessions (AKA, "interviews").
  - Reporting the FAR groups and personnel to the SEI.

# Technique 4: Cover Identities

- Protecting the identities in this scenario is straightforward.
- Personnel being interviewed should use their cover identities when working with the appraisal team.
- Cover identities should be reported with respect to the FAR groups and personnel in SAS.
- The DARK KNIGHT program should maintain a classified mapping of cover identities to actual identities so that consistent cover identities may be used for any appraisal follow-up activities.

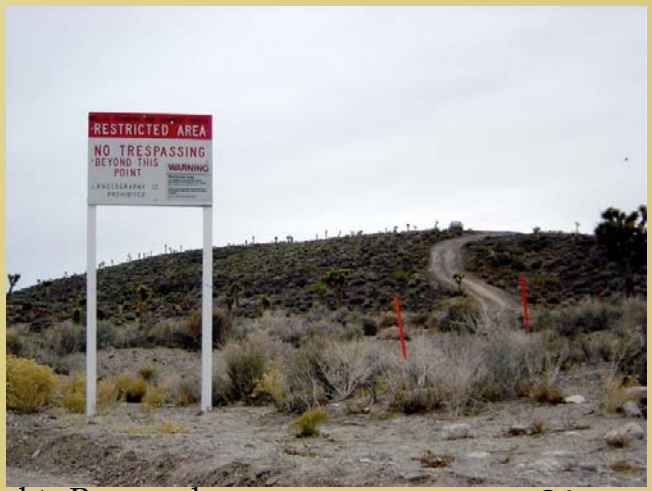

# Scenario 4: Undisclosed Locations and Customers

- Our story:
  - For almost 50 years, the US government has been holding Technical Exchange Meetings at a military base in southern Nevada with a mysterious group known as the Vulcans.
  - Contrary to the apocryphal claims about the invention of the Internet, the Vulcans, in fact, supplied the US government with the key concepts.
  - The Vulcans have been watching the development of the CMMI and now believe an appraisal of their processes would assist in their next project, known as TRANSPORTER.
    - The Vulcans believe that TRANSPORTER will help relieve the hassles of modern airline travel.
  - Although the US government has agreed to request the SEI conduct this appraisal, the association of the project with the Vulcans or with southern Nevada is classified.

Business Transformation Institute

# Appraising TRANSPORTER

- The restrictions of scenarios 1, 2, and 3 probably apply here!
  - We consider only the undisclosed location and customer aspect.
- The key challenge in appraising TRANSPORTER will be in concealing details of who and where.
- The most difficult aspects of this challenge are:
  - Disassociating the program from the location.
  - Disassociating the program from the customer.



# Hiding the Details

- Presuming that the techniques of handling classified information and identities from scenarios 1, 2, and 3 are effective, managing scenario 4 involves:
  - Identifying a plausible alternative location for the program that may be used for the claimed work location.
  - Identifying a plausible alternative affiliation for the program that may be used for the organizational unit.
- The alternative location and affiliation are sufficient for SAS.
  - Since the true organizational unit and location cannot be disclosed, there will be little benefit to publishing the appraisal results to PARS.


# Conclusions

- Many of the challenges faced in appraising programs that are classified can managed, given careful planning.
- A cleared mini-team with access to the program may be important.
- Communicating with and getting the cooperation of security, perhaps with the intercession of the appraisal sponsor, is critical.
- Be sure to check “Sensitive Program” in SAS to indicate that some details may not be subject to disclosure.