



DEPARTMENT OF THE NAVY
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH, DEVELOPMENT AND ACQUISITION
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

FEB 20 2008

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Required Use of Standardized Process for the Identification of Critical Program Information (CPI) in DON Acquisition Programs

Reference: (a) DoD Directive 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection", 10 Sep 97 (currently under revision)
(b) SECNAVINST 5000.2C, "Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System", 19 Nov 04
(c) DoD Instruction 5000.2, "Operation of the Defense Acquisition System", 12 May 03

The protection of Department of the Navy (DON) sensitive technologies is critical to maintaining the US advantage on both the current and future battlefields. Reference (a) requires all DoD acquisition Program Managers to identify CPI that may be contained in their program early in the acquisition life cycle (not later than Milestone (MS) A or when the program enters the acquisition process). In addition to the conventional ACAT I-IV acquisition programs, this requirement also applies to Abbreviated Acquisition Programs, Technology Spirals, and advanced programs that have potential for early deployment.

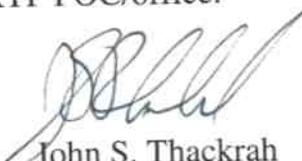
Previously, no DON standardized process existed for use in evaluating programs for the presence of CPI. In early 2007, representatives from the four major DON acquisition SYSCOMS (NAVSEASYSKOM, NAVAIRSYSKOM, SPAWARSYSKOM, and MARCORSYSKOM) conducted a Lean Six Sigma/ Kaizen event with the goal of developing a standardized DON CPI Identification Process. The initial process was subjected to pilot programs by the SYSCOMS and modified where appropriate.

This process will be integrated into DON policy documents as appropriate. As part of the DON Acquisition Community's process improvement efforts, Enclosure (1) sets forth the standardized process that PMs will now be required to utilize when identifying CPI in their respective acquisition programs. For

SUBJECT:: Required Use of Standardized Process for the Identification of
Critical Program Information (CPI) in DON Acquisition Programs

consistency, the requirement to use this approved process applies to both government employees and contractors supporting DON acquisition programs in this area. Consistency is vital to enable horizontal protection of programs among the PEOs, SYSCOMs and across the DoD.

The process will be reviewed, and updated, if appropriate, on an annual basis by the SYSCOM Research and Technical Protection (RTP) Points of Contact (POCs). The ASN (RDA) Chief Systems Engineer will approve any changes/updates to this process. Questions concerning this matter should be directed to the appropriate SYSCOM RTP POC/office.



John S. Thackrah
Acting

Attachments: As stated.

Distribution:

COMNAVSEASYS
COMSPAWARSYS
COMNAVAIRSYS
COMMARCORSYS
RDA CHSENG
DASN (IP)
DASN (A&LM)
DASN (M&B)
DASN (SHIPS)
DASN (AIR)
DASN (C4I/SPACE)
DASN (IWS)
DASN (ExW)
PEO (IWS)
PEO (SHIPS)
PEO (LMW)
PEO (CARRIERS)

SUBJECT:: Required Use of Standardized Process for the Identification of
Critical Program Information (CPI) in DON Acquisition Programs

PEO (SUBS)
PEO (U&W)
PEO (A)
PEO (T)
PEO (C4I)
PEO (SPACE SYS)
PEO (EIS)
PEO (LS)
PEO (JSF)
ONR

Copy to:
DIRNCIS

Standard Operating Procedures (SOP)
for the
**Standardized Critical Program Information
Identification Process**
in
Department of Navy Acquisition Programs

Version 1.01

26 Sep 2007

INTRODUCTION

The attached document outlines the standard and approved process for use by both Department of Navy (DON) employees and contractors involved in the identification of Critical Program Information (CPI) in DON acquisition programs (to include conventional ACAT I-IV programs, Abbreviated Acquisition Programs, Technology Spirals, and advanced programs that have potential for early deployment). This process was developed through a Lean Six Sigma (LSS) collaborative effort involving the DON Acquisition commands, including process pilots run at various Program Executive Offices (PEOs) within the DON Acquisition community. It is the first formal DON-wide process to be utilized by those personnel responsible for or tasked with CPI identification. The process itself is collaborative in nature, involving both those personnel that are experts on a program's technology and those that are experts on protecting technologies. The process calls for the formation of a multi-disciplinary Integrated Product Team (IPT) comprised of representatives from the acquisition, engineering, Research Technology Protection (RTP) (e.g. Security, Operations Security (OPSEC), Anti-Tamper (AT) and Threat/Intelligence support)), Foreign Military Sales (FMS)/Foreign Disclosure Office (FDO) and Counterintelligence (CI) fields. The time and effort required by a program to complete the CPI identification process is highly dependent upon the program's size and complexity, as well as its commitment of the necessary personnel to participate in the process. The attached SOP is intended to be used as a guide through the CPI identification process. It is not intended to be the sole guidance or information source for personnel completing the process. Personnel completing the CPI identification process should not start or attempt the process without direct involvement and assistance of the appropriate SYSCOM RTP representative. Only after CPI is determined to be present or not present can a Program Protection Plan (PPP) or Abbreviated PPP (APPP) be developed and additional guidance provided, outside the process prescribed in this SOP.

The CPI identification process is broken down into the following seven steps: Phase 1-Request Validation; Phase 2- Team Selection; Phase 3-Team Training; Phase 4- External Review; Phase 5-Internal Review; Phase 6- Candidate CPI List; and Phase 7-Final CPI List. Each of these phases is explained in detail as you follow the attached SOP.

There are several roles that have varying degrees of responsibility and actions throughout the process. Each role or 'swim lane' is described briefly below:

Program Manager (PM): Primarily responsible for assigning a Program Office Protection Lead (POPL), making personnel available for participation in the process, and approving process results, or referring back to IPT for further analysis.

Program Office Protection lead (POPL): This moniker is unique to this process and is used to describe the individual (government, contractor or military) that is assigned by the program as the primary POC for the process and responsible for carrying out or coordinating the duties described in the process, tracking and documenting progress, and preparing and presenting process results to the PM.

RTP Security Personnel: This is the supporting SYSCOM individual who will be the primary POC for working the process with the program. They may be a subject matter expert from several disciplines to include Security, Operations Security, Anti-Tamper or Threat/Intelligence Support. They are the program's source for information on the process or CPI, work closely with the POPL and serve an active role throughout the process.

Lead Engineer, SW/HW Engineer, Technical Experts, etc.: These personnel are the programs Subject Matter Experts and also may be assigned as participants in the IPT. They will be completing a survey questionnaire (through one of three methods described infra), providing expertise in their areas during discussions and vetting of candidate CPI, and serve an active role throughout the process.

FMS/FDO: SYSCOM personnel facilitating the transfer of U.S. information on programs to foreign governments or entities through U.S. Government sanctioned sales or information exchanges. These personnel support the process through expertise in foreign information exchange matters and potential foreign interests in program information.

NCIS/Threat Support: There are two supporting efforts in this area. There are Navy Criminal Investigative Service (NCIS) special agents and intelligence analysts, who are the DON's Counterintelligence support providers, and other threat support providers (ONI, DIA, etc.) which are coordinated through the SYSCOM Scientific and Technical Intelligence Liaison Officer (STILO). Both areas support the process through counterintelligence or technology threat assessments respectively, as well as providing expertise on foreign efforts or interests in U.S. program's technologies or information.

A list of Acronyms used in this document is located at the end of this SOP.

BACKGROUND

The protection of the Department of the Navy (DON) sensitive technologies is critical to maintaining the US advantage on both the current and future battlefields. Toward that end, Department of Defense (DoD) Directive 5200.39 requires all DoD acquisition programs to identify Critical Program Information (CPI) that may be contained in each program. DoD Directive 5200.39 further directs that CPI must be identified early in the acquisition life cycle (not later than Milestone (MS) A or when the program enters the acquisition process). Program Managers (PMs) are responsible for ensuring all programs are evaluated for CPI and completing the Program Protection Plan where required.

This document provides the standardized process that DON personnel or contractors responsible for or tasked with the identification of CPI will now be required to utilize for their respective acquisition programs. There are seven steps in the process, a brief explanation of each step follows:

Phase 1- Request Validation

During this phase, it is determined if the program meets the necessary criteria for CPI evaluation. This phase starts the process by the initiation of contact from the Program Office Protection Lead (POPL) to the SYSCOM RTP representative. This phase is completed by the SYSCOM RTP Security representative with the assistance of the POPL utilizing the CPI Validation Tool contained in the SOP. If the determination is made that the program's request is valid, the process moves to the next phase. The CPI Validation Tool must be completed by a SYSCOM RTP representative for its results to be considered valid.

Phase 2- Team Selection

The Team Selection phase ensures that the appropriate personnel are included in the CPI IPT. The SYSCOM RTP security representative will provide advice on the make-up of the IPT and the process Tools. Once the team has been selected, the IPT members will be provided with the Tools and other training materials to be used in the next phase. It is ultimately the PM's responsibility to ensure the IPT is comprised of appropriate representatives.

Phase 3- Team Training

The purpose of this phase is to train the IPT participants on the process and expectations on what will be accomplished. Training on the definition of CPI, potential indicators of CPI, and process Tools will be included. Conduct and documentation of the training is the responsibility of the POPL in coordination with the SYSCOM RTP security representative.

Phase 4- External Review

This is the first step in the review and evaluation of program data and technology. During this phase, the POPL gathers the relevant program documentation and distributes it to the IPT with the purpose of determining primarily external information sources that may affect Candidate CPI (C-CPI). A list of the suggested external information sources is included in the SOP.

Phase 5- Internal Review

The Internal Review phase is the second part of the evaluation of the program's data and technology for the presence of CPI. This review uses the information compiled during the previous External Review phase to compare program data or technologies against specific CPI criteria in order to develop a list of C-CPI.

Phase 6- Candidate-CPI List

Following compilation of a C-CPI list, the IPT in conjunction with other interested parties (FDO/FMS, NCIS) are tasked to reach agreement on the C-CPI list. This list will form the basis for the selection of the final CPI.

Phase 7- Final CPI List

The final phase of the CPI identification process involves securing agreement from the Program Manager (PM) on the final CPI list. Utilizing the list of C-CPI developed in the previous phase, the POPL engages with the PM and obtains approval on the CPI list. If PM approval is not obtained, the effort returns to the previous phase for re-work of the C-CPI list.

This Standard Operating Procedure (SOP) will define the activities and tools to be used during each of the phases to ensure consistent execution is maintained across all DON activities performing CPI evaluations. A CPI Primer is provided as Appendix A.

The Department of the Navy (DON) standardized Critical Program Information (CPI) Identification Process is performed in seven phases. These phases are presented as an overview in Figure 1 below and are detailed throughout the rest of this SOP.

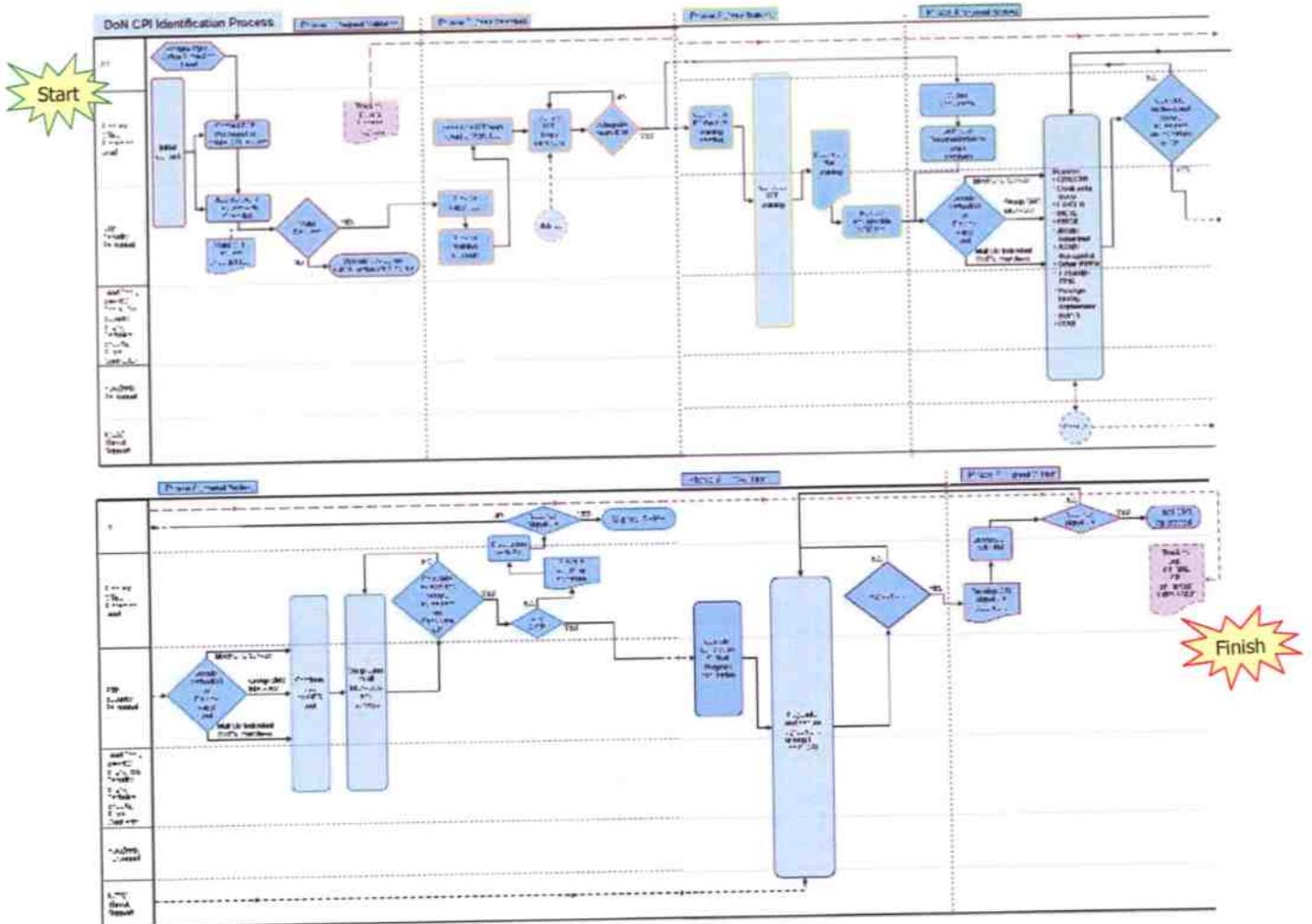
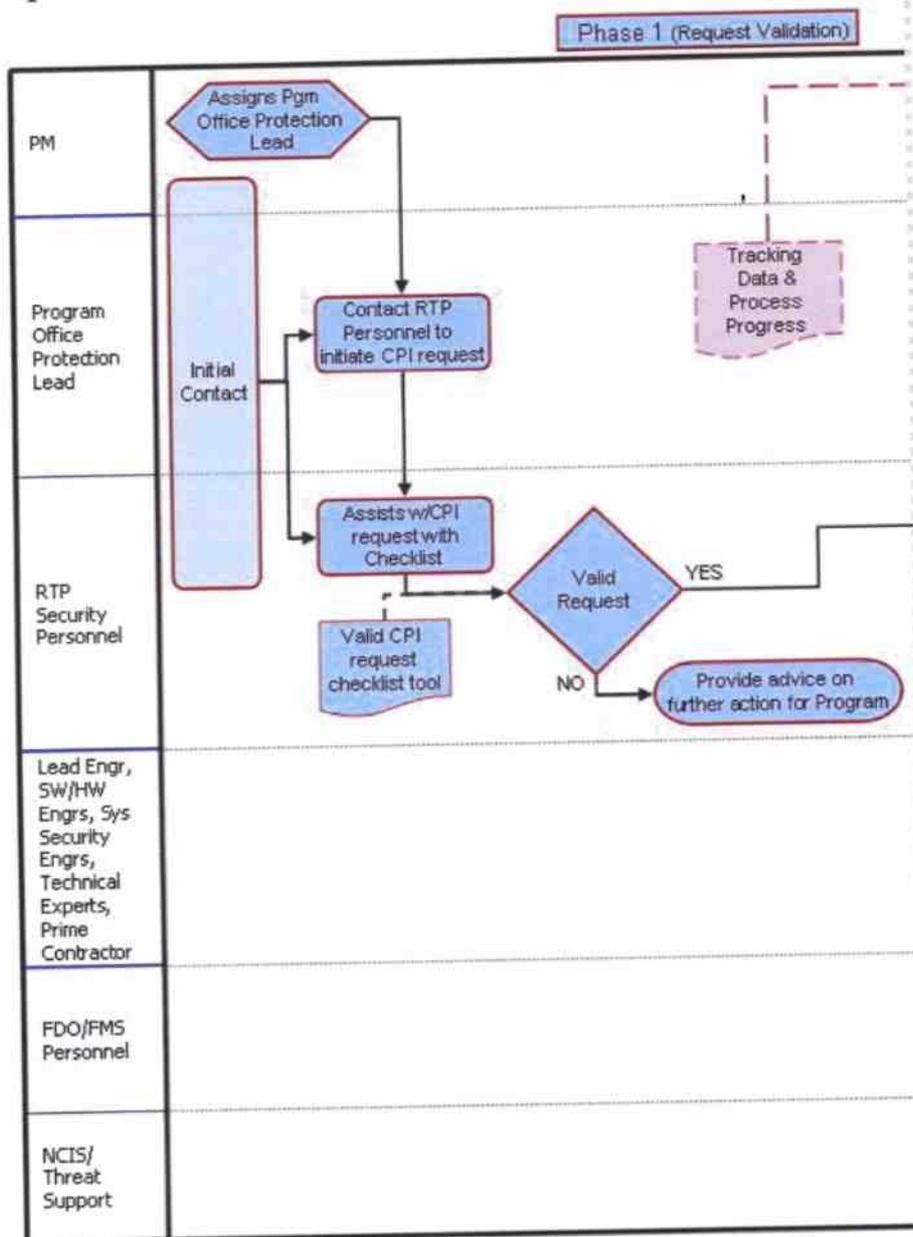


Figure 1: DON Standard CPI Identification Process Overview

The phase titles are self descriptive and are as follows:

1. Request Validation
2. Team Selection
3. Team Training
4. External Review
5. Internal Review
6. Candidate CPI (C-CPI) List
7. Final CPI List

Phase 1: Request Validation:



The "Request Validation" phase is intended to determine whether or not a request for a program to complete the CPI Identification Process is valid (necessary), based on standard DON criteria. During the request validation phase the program office contacts their System Command (SYSCOM) Research Technology Protection (RTP) security personnel to verify the need for determining if a program has CPI. This determination must be made by the RTP security personnel and not by the Program. The individual who will be assigned by the Program as the Program Office Protection Lead (POPL) usually makes this contact. Once RTP security personnel have been contacted, they work with the POPL, using the CPI validation tool (Appendix B), to determine whether there is a valid CPI Identification request. If completion of the CPI Validation Tool indicates the CPI Identification request is not valid the RTP security

personnel will provide advice to the program office on any required further action. If the completed CPI Validation Tool indicates a valid CPI Identification request, the process continues to the "Team Selection" phase.

SYSCOM RTP security personnel may be contacted via the respective SYSCOM security Offices.

The Program Office Protection Lead is responsible for:

- Contacting the SYSCOM RTP security personnel.
- Being prepared to answer at least the following questions:
 - Is this an Acquisition Program?
 - Is the program at or is it pre Milestone (MS) A, B, or C?
 - Is there an Engineering Change Proposal (ECP) / Initial Capabilities Document (ICD) change planned or a Critical Design Review (CDR) coming up?
 - Is the equipment 100% Commercial off the Shelf (COTS) or not?
- Begin use of the CPI data tracker tool (Appendix C) once supplied by the RTP security personnel.

The SYSCOM RTP security personnel are responsible for:

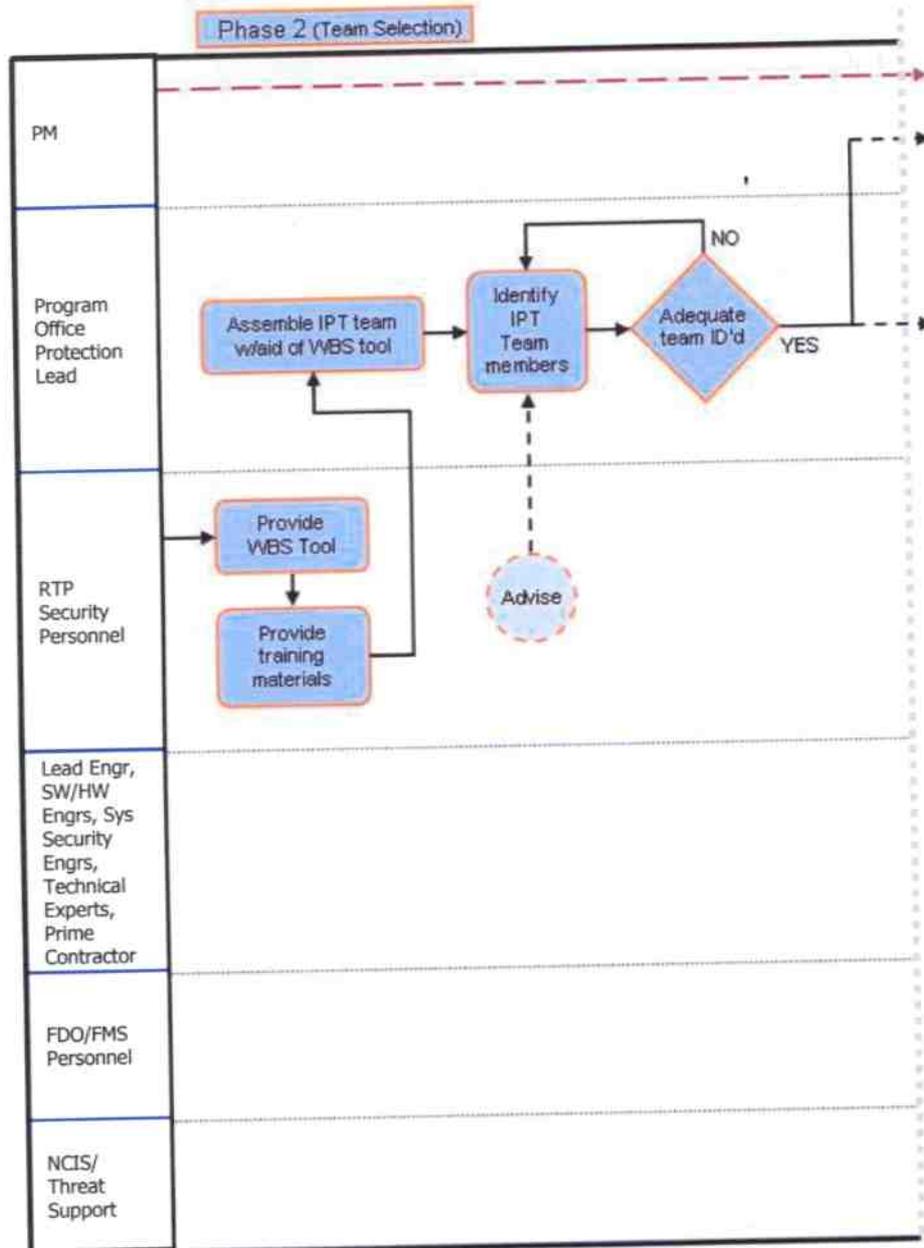
- Asking the questions identified in the CPI Validation Tool and interpreting responses.
- Making the determination on starting the CPI Identification Process.
- Documenting the data for the CPI Validation Tools used on a quarterly basis and providing that data to the process owner.
- Completes applicable sections of the CPI data tracker tool, prepares and provides the data tracker for use by the POPL.

At this point tracking data and process progress data are initiated. The RTP security personnel will collect the following data for all CPI Validation Tools performed:

Date of Request
Date of Decision
Length of call (min)
Yes, # No, RFI
Why No?
Late Starts
Date WBS Requested
WBS Tool Provided? Y/N? Date

The CPI Validation Tool is presented in Appendix B. The CPI Data Tracker Tool format / inputs are identified in Appendix C.

Phase 2: Team Selection:



The “Team Selection” phase is intended to provide the Program Office Protection Lead (POPL) with the process tools that will be used throughout the completion of the process and determine the appropriate personnel to participate in the process. At the initiation of the team selection phase the RTP security personnel will provide the Work Breakdown Structure (WBS) Tool, CPI Data Tracker Tool and related training materials (SOP, acronym list and CPI process swim lane) to the POPL. With the aid of the WBS Tool the POPL assembles the Integrated Product Team (IPT) to be used on the CPI Identification Process. Participants should include the program lead engineer, software and/or hardware engineers, system security engineers, various technical experts, and the program contractor. The RTP security personnel provide advice to the POPL on

the make-up of IPT membership as the IPT is formed. Team selection continues until the appropriate IPT composition is established. Once the team is formed the "Team Training" phase can begin.

The Program Office Protection Lead is responsible for:

- Incorporating/populating the WBS Tool.
- Assigning appropriate Points of Contact (POCs) and IPT, members.
- Providing the WBS Tool back to the RTP security personnel.
- Requesting advice from the RTP security personnel on the IPT membership makeup (types of people).
- Advising the Program Manager (PM) on the size of the IPT, the required resources and status on the CPI Identification Process.
- Discussing any issues on process completion with the PM.
- Continued use of the data tracker to capture the required data for metrics.

The RTP security personnel are responsible for:

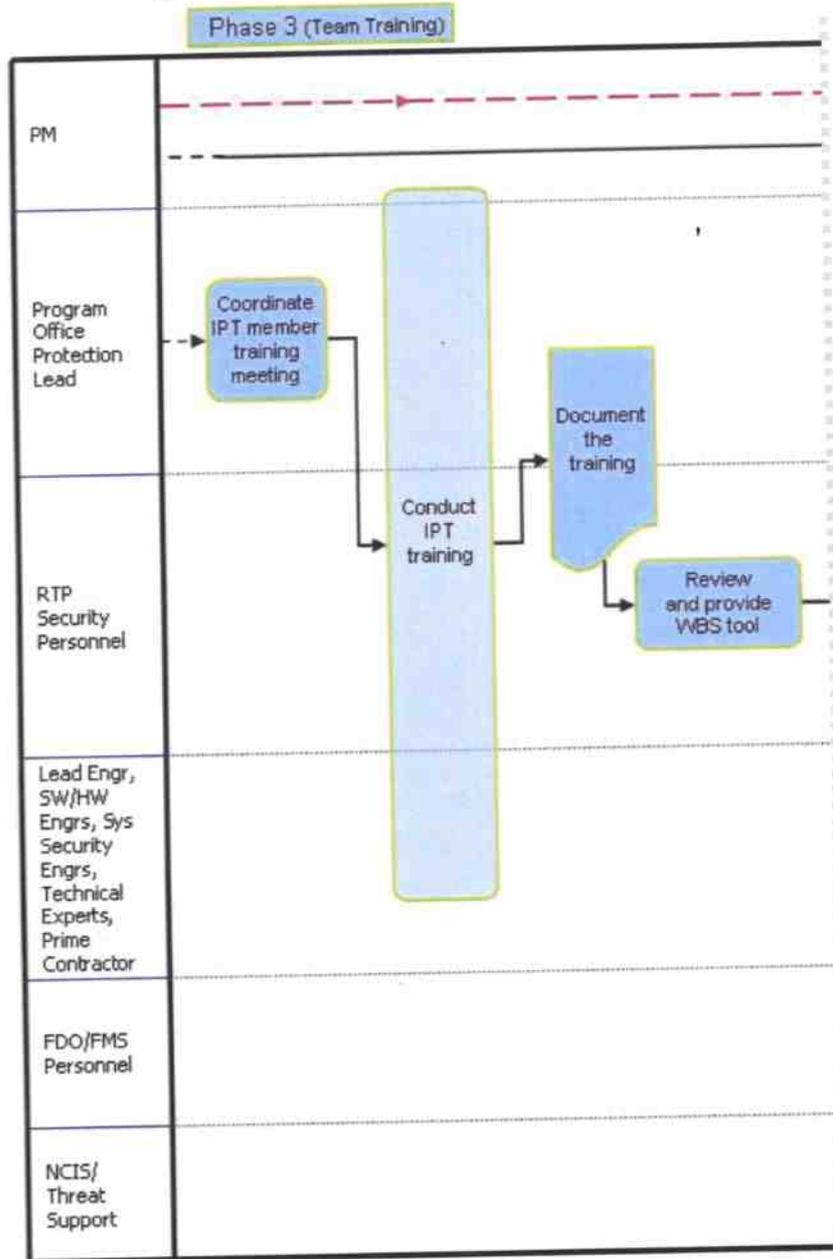
- Providing a blank WBS Tool, CPI Data Tracker Tool and training materials (SOP and Acronym list and Process swim lane) to Program Office Protection Lead.
- Advising the Program Office Protection Lead on the make-up of the IPT membership.

The IPT is responsible for participating in the CPI Identification Process, as required.

During this phase the program office is responsible for providing adequate resources to support IPT formation and their associated efforts.

CPI Data Tracker metrics to be collected during this phase includes the start date and a WBS Tool that is populated with IPT membership. This information is also part of what is provided quarterly to the CPI process owner.

Phase 3: Team Training:



The “Team Training” phase is intended to train the process participants on the process itself and what is expected as a result of the process completion. Training will also as a minimum include the definition of CPI, potential indicators of CPI and the use of the WBS Tool. This phase involves the Program Office Protection Lead (POPL) coordinating and documenting the team training session, the IPT team participating in the training, and the POPL and RTP security personnel updating the WBS Tool to initiate the CPI evaluation.

The Program Office Protection Lead is responsible for:

- Coordinating the IPT training.
- Ensuring the training is completed with help of RTP security personnel.
- Documenting the training.
- Continued use of the data tracker to capture the required data for metrics.

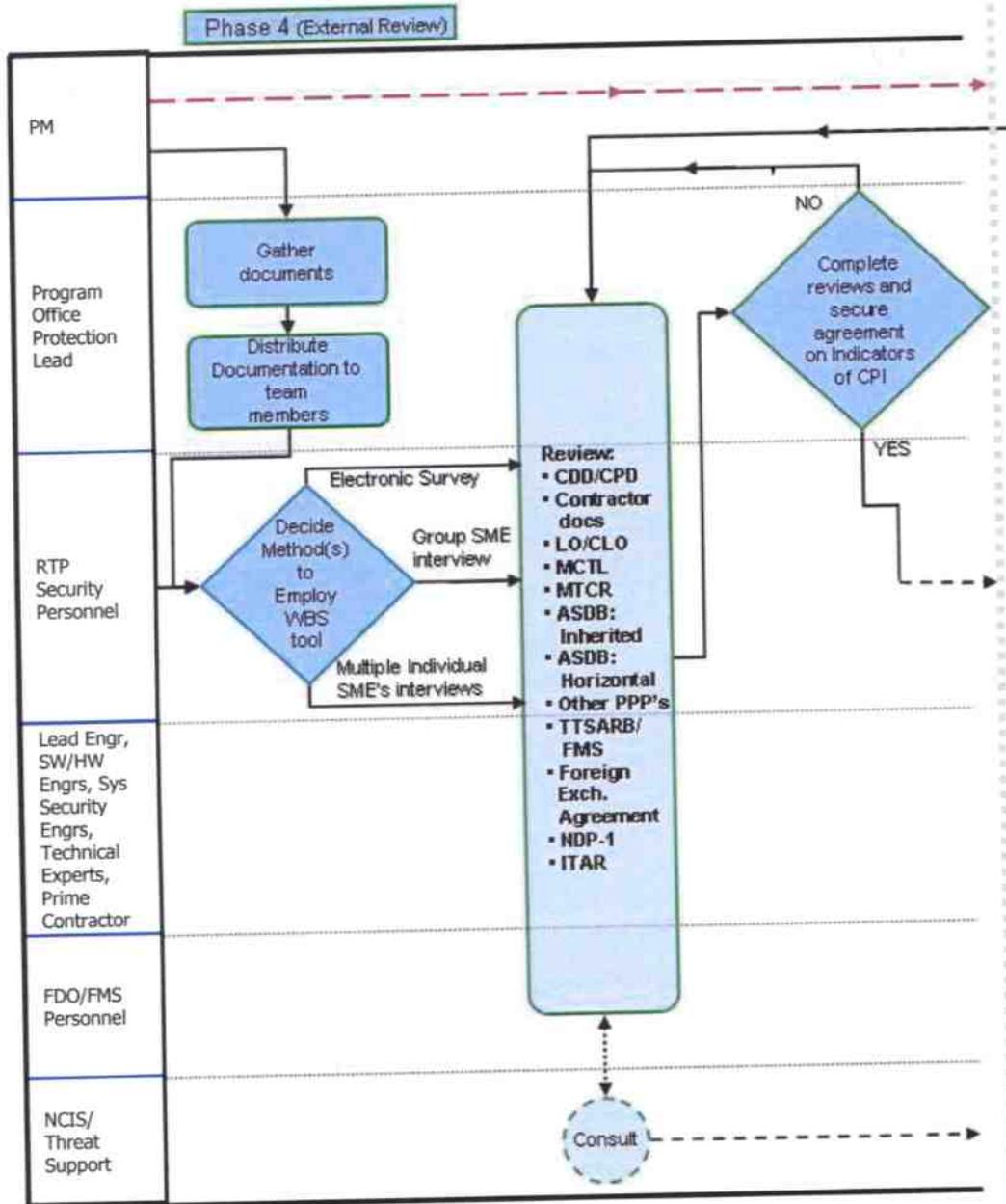
The RTP security personnel are responsible for:

- Providing, assisting with and/or performing the necessary training.
- Ensuring the training is documented.
- Updating the WBS Tool for use during the CPI evaluation.

IPT members are responsible for participating in the training.

CPI Data Tracker metrics to be collected during this phase includes team size and date team training was completed.

Phase 4: External Review:



The "External Review" phase is the first phase where data about the program's technology is evaluated and documented, based on resources and requirements that are external to the program itself. This phase is the first significant event associated with CPI Identification Process. A critical part of this phase includes the SMEs placing their input and analysis of a program into the WBS tool. The WBS Tool must be completed by the SMEs for its results to be considered valid. During this phase the Program Office Protection Lead (POPL) gathers the relevant documentation and distributes it to the IPT. Once documentation is available the POPL, the IPT, the RTP security personnel, and the Foreign Disclosure Officer (FDO)/Foreign Military Sales (FMS) personnel review the information for indicators of CPI. Naval Criminal Investigative

Service (NCIS) and related threat support organizations support the external review in a consultation capacity. Once the review is complete the POPL secures agreement on the indicators of CPI. If agreement can not be reached, documentation review will continue to ensure all potential indicators of CPI have been defined. With indicators of CPI identified the process proceeds to the internal review phase.

In association with the execution of this phase the DoD Anti-Tamper Critical Technology (CT) Tool should be used. This tool enables efficient key-word searches of the Low Observable (LO)/Counter-Low Observable (CLO), Militarily Critical Technologies List (MCTL) and Missile Technology Control Regime (MTCR). Use of this tool will significantly decrease the time required to review these reference documents. The CT Tool is classified SECRET and can be obtained from the SYSCOM RTP security personnel.

The Program Office Protection Lead will be responsible for:

- Locating the review documentation.
- Distributing the documentation or identifying where it can be obtained.
- Ensuring the reviews are completed and the results are documented in the external review portion of the WBS Tool.
- As Assigned:
 - Review CDD/ CPD
 - Review LO / CLO
 - Review MCTL
 - ASDB: Horizontal
 - TTSARB / FMS Review
 - NDP-1
 - Review Contract Documents
 - Review MTCR
 - ASDB: Inherited
 - Other PPP
 - Foreign Exchange Agreement
 - ITAR
- Continued use of the data tracker to capture the required data for metrics.

The RTP security personnel will be responsible for:

- Determining the method to be used to conduct the external review.
- Assisting with the reviews.
- As Assigned:
 - Review CDD/ CPD
 - Review LO / CLO
 - Review MCTL
 - ASDB: Horizontal
 - TTSARB / FMS Review
 - NDP-1
 - Review Contract Documents
 - Review MTCR
 - ASDB: Inherited
 - Other PPP
 - Foreign Exchange Agreement
 - ITAR
- Ensuring results are documented in the external review portion of the WBS Tool

The IPT will be responsible for:

- Participating in their respective areas of expertise.
- As Assigned:
 - Review CDD/ CPD
 - Review LO / CLO
 - Review MCTL
 - ASDB: Horizontal
 - TTSARB / FMS Review
 - NDP-1
 - Review Contract Documents
 - Review MTCR
 - ASDB: Inherited
 - Other PPP
 - Foreign Exchange Agreement
 - ITAR
- Ensuring they document results in the external review portion of the WBS Tool

FDO/FMS personnel will be responsible for:

- Participating in their respective areas of expertise.
- As Assigned*:
 - Review LO / CLO
 - Review MCTL
 - Foreign Exchange Agreement
 - ITAR
 - Review MTCR
 - TTSARB / FMS Review
 - NDP-1
- Ensuring results are documented in the external review portion of the WBS Tool.
*Completion of above might require review for information in the CDD/CPD and contract documents.

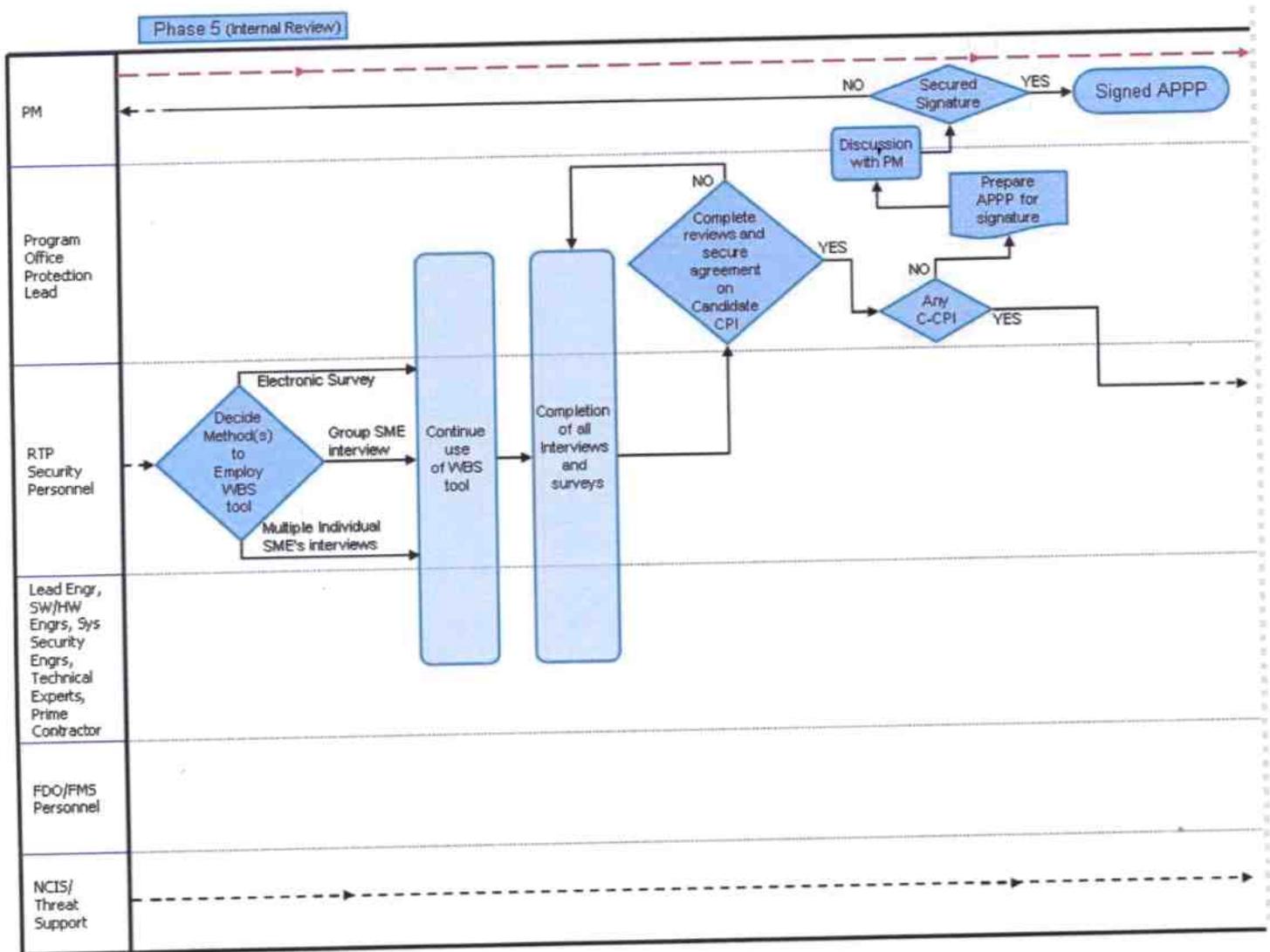
NCIS/Threat support organizations:

- Will provide consultation when requested/required.

Data collection during this phase will include completing the External review portion of the WBS Tool and maintaining the CPI process data tracker. CPI data trackers metrics to be captured include:

- Start of EXT Review
- End of EXT Review
- # People Involved
- Average Time involved per person
- # of CPI Indicators
- # Of WBS line items (total)

Phase 5: Internal Review:



The “Internal Review” phase is the second half of the CPI identification effort where the programs technology is evaluated and documented. These efforts focus on the internal review of indicators of CPI. A critical part of this phase includes the SMEs placing their input and analysis of a program into the WBS tool. The WBS Tool must be completed by the SMEs for its results to be considered valid. The RTP security personnel take the data collected in the WBS Tool during the external review and perform interviews of various program Subject Matter Experts (SMEs) to develop a Candidate CPI (C-CPI) list. Interviews can be performed via electronic survey, through group SME interviews or by using multiple individual SME interviews. The RTP security personnel, with the participation of the Program Office Protection Lead (POPL) and the IPT, will base the interviews on the WBS Tool and will compile the interview results to establish the C-CPI. This C-CPI list will be provided to the POPL for concurrence. If concurrence can not be reached the interviews data and C-CPI list will revisited. Once the reviews have been completed and agreement secured on the C-CPI the process proceeds with CPI compilation. If no C-CPI are identified, the POPL will prepare an Abbreviated Program

Protection Plan (APPP) for signature. The APPP will be discussed with the Program Manager (PM) and recommended for signature. If the PM concurs with the 'no-C-CPI' results and signs the APPP, the CPI Identification Process is complete. If the PM does not concur with the 'no CPI' determination and does not sign the APPP, the CPI identification efforts return to the phase four External documentation review and Internal review for further analysis. This process continues until the PM is satisfied with the CPI identification efforts and agrees to the 'any C-CPI' decision.

The Program Office Protection Lead will be responsible for:

- Continued use of the WBS Tool to conduct the Internal reviews per the advice of the RTP security personnel.
- Securing agreement with IPT on C-CPI.
- Documenting the identified C-CPI in the WBS Tool.
- Continued use of the data tracker to capture the required data for metrics.
- If no C-CPI is identified, the Program Office Protection Lead will prepare an APPP with RTP security personnel assistance and present it to the PM for signature.
- If APPP is signed:
 - provide RTP security personnel a signed copy
 - upload APPP into the ASDB
 - return completed data tracker to RTP security personnel.
- If APPP is not signed, continue CPI Identification process.

The RTP security personnel will be responsible for:

- Determining the method to be used to conduct the Internal review.
- Assisting with the interviews/interview reviews.
- If no C-CPI are identified, the RTP security personnel will:
 - assist with APPP development.
 - Ensure upload of the finalized APPP into the ASDB.
 - Ensuring the data tracker is returned by the POPL and complete.
 - Complete the CPI Identification Process metrics.

The IPT will be responsible for:

- Participating in their respective areas of expertise in the Internal review.
- Documenting the identified Candidate CPI in the WBS Tool.

The PM, if presented with an APPP, is responsible for determining agreement and signing.

NCIS/Threat support organizations:

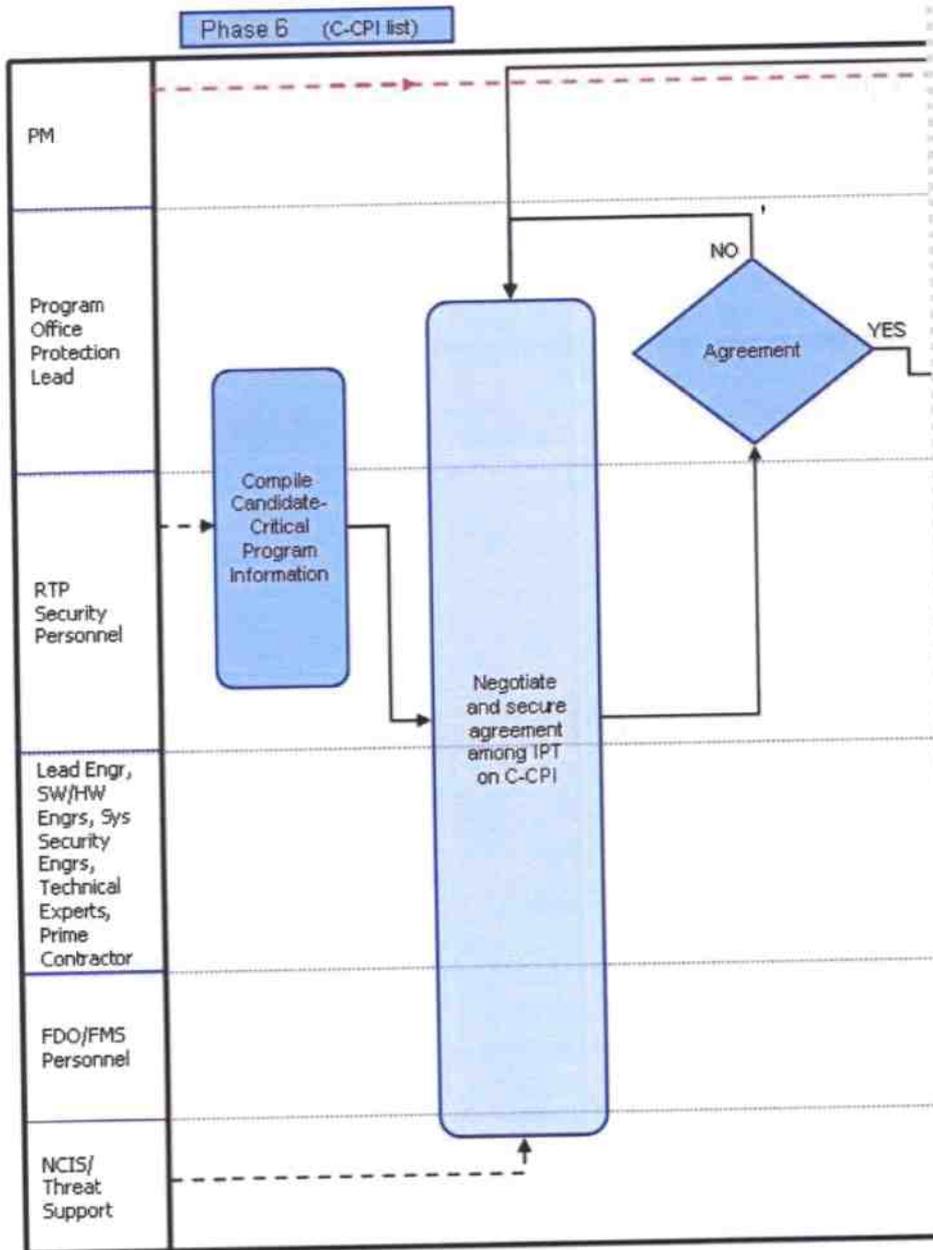
- Will continue to provide consultation when requested/required.

Data collection during this phase will include completing the internal review portion of the WBS tool and maintaining the CPI process data tracker. CPI data trackers metrics to be captured include:

Start of Internal Review

End of Internal Review
People Involved
Average Time Involved
of CPI Indicators
No CPI found

Phase 6: Candidate Critical Program Information List:



The “C-CPI List” phase is utilized to finalize those indicators of CPI that were developed during the previous phases. Using the C-CPI identified in phase five the Program Office Protection Lead (POPL) and RTP security personnel compile all C-CPI information and negotiate with the IPT, FDO/FMS personnel and NCIS/related threat support organizations to secure agreement on C-CPI. Discussions continue until agreement on the C-CPI can be reached. Once all participants concur, the C-CPI list proceeds to finalization.

The Program Office Protection Lead will be responsible for:

- Preparing the list of Candidate CPI.
- Gaining agreement from the IPT/RTP POCs.
- Continued use of the data tracker to capture the required data for metrics.

The RTP security personnel, IPT, and FDO/FMS personnel are responsible for supporting the Program Office Protection Lead as required.

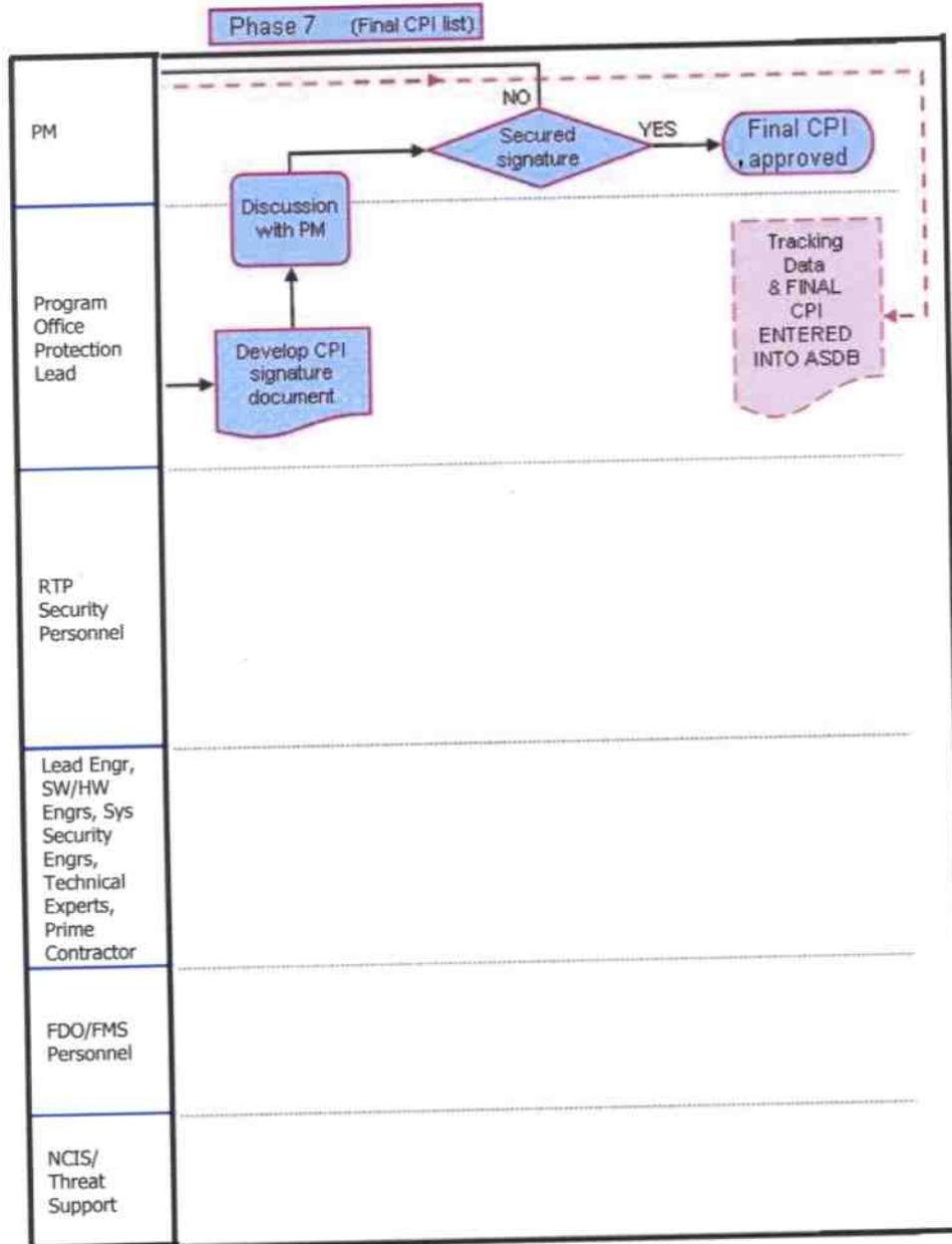
NCIS/Threat support organizations:

- Will continue to provide consultation when requested/required.

Data collection during this phase will consist of completing the WBS Tool and maintaining the CPI process data tracker. CPI data trackers metrics to be captured include:

- Start Compile of C-CPI List (Date)
- Obtain Agreement of C-CPI List (Date)

Phase 7: Final Critical Program Information List:



The “Final CPI List” phase completes the CPI process by finalizing the CPI list and securing agreement to it by the PM. Using the C-CPI list established during phase six the Program Office Protection Lead (POPL) will develop the CPI signature document and discuss this document with the PM. Once completed the document is provided to the PM for signature and final CPI approval. If the PM does not sign the final CPI list the effort returns to the C-CPI negotiation process for modifications.

The Program Office Protection Lead is responsible for:

- Developing the CPI signature document.
- Discussing the CPI signature document with PM and securing the PMs signature.
- Completing the CPI Data Tracker Tool spreadsheet.
- Completing the WBS Tool.
- Providing the completed WBS Tool, CPI Data Tracker Tool and signed final CPI list to the RTP security personnel POC.
- Uploading the finalized CPI into the Acquisition Security Database (ASDB).

The RTP security personnel are responsible for:

- Supporting the POPL as required.
- Ensuring upload of the finalized CPI into the ASDB.
- Ensuring the data tracker tool is returned by the POPL and complete.
- Completing the CPI Identification Process metrics.

The IPT is responsible for supporting the POPL as required.

The Program Manager is responsible for approving the CPI list or advising the POPL on why not.

NCIS/Threat support organizations are to standby for the Threat Assessment request.

Data collection during this phase will include completing the WBS Tool and closing the CPI process data tracker tool. CPI data trackers metrics to be captured include:

- CPI list signed - Yes, No and Why Not?
- Date ASDB update completed
- Cycle time for CPI ID
- Cost

Process ends with the approval of the CPI list by the PM and the compilation of the CPI Identification Process metrics.

Acronyms

ACAT	Acquisition Category
APPP	Abbreviated Program Protection Plan
ASDB	Acquisition Security Database
Acq	Acquisition
AT	Anti-Tamper
BB	Blackbelt
C & E	Certification & Evaluation
C/A	Certification and Accreditation
C-CPI	Candidate Critical Program Information
CDD	Capability Development Document
CDR	Critical Design Review
CNO	Chief of Naval Operations
COTS	Commercial off the Shelf
CPD	Capability Production Document
CPI	Critical Program Information
CT	Cycle Time
DCID	Director of Central Intelligence Directive
DoD	Department of Defense
DON	Department of the Navy
DPM	Deputy Program Manager
ECP	Engineering Change Proposal
Engr	Engineer
Exch.	Exchange
EXCOM	Executive Committee
EXT	External
FAR	Federal Acquisition Regulation
FDO	Foreign Disclosure Officer
FMEA	Failure Mode and Effects Analysis
FMS	Foreign Military Sales
HUMINT	Human Intelligence
HW	Hardware
IA	Information Assurance
ICD	Initial Capabilities Document
ID	Identification
IMINT	Imagery Intelligence
IPT	Integrated Product Team to identify CPI, for example; Lead Engr, SW/HW Engrs, Sys Security Engineers, Tech Experts, Pgrm Contractor
ITAR	International Traffic in Arms Regulation
KPP	Key Performance Parameters

LO/CLO	Low Observable/Counter-Low Observable
MCTL	Militarily Critical Technologies List
MS	Milestone
MTCR	Missile Technology Control Regime
NCIS	Naval Criminal Investigative Service
NDP-1	National Disclosure Policy-1
NSA	National Security Agency
OPSEC	Operations Security
OSINT	Open Source Intelligence
PCT	Process Cycle Time
PERSEC	Personnel Security
Pgrm	Program
PM	Program Manager
POC	Point of Contact
POPL	Program Office Protection Lead
PPP	Program Protection Plan
Prog.	Program
RCA	Root Cause Analysis
RFI	Request for Information
RPT	Report
RTP	Research Technology Protection
SCG	Security Classification Guide
SIGINT	Signal Intelligence
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SOW	Statement of Work
SW	Software
Sys	System
Tech	Technology
TTSARB	Technology Transfer Security Assessment Review Board
WBS	Work breakdown structure or any list that defines the product being procured that will be useful in determining CPI

Appendix A - Critical Program Information Primer

The following guidelines should assist you in understanding what Critical Program Information (CPI) is and whether your program may have CPI. This guide is not intended as the determining factor of whether or not information is potential or actual CPI. It is intended for educational purposes to provide basic information and guidance on CPI. In order to determine whether or not a program has CPI, an assessment for CPI, conducted through the DON's CPI Identification Process, must be completed. The Program Manager (PM) must identify CPI no later than milestone A and reevaluate it prior to each Milestone thereafter, per DoD Directive 5200.39, *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*. CPI is basically defined as information, technologies, or systems that if compromised will cause:

- Significant alteration of program direction
- Compromise the program or system capabilities
- Shortened expected combat-effective life of the system
- Additional RDT&E resources to counter the impact of the CPI compromise

You should consider not only classified information, but also unclassified information within your programs, technologies, or systems in making your determination. The classification of information does not determine whether or not it's CPI. Some examples of CPI may include the following:

- Program vulnerabilities / countermeasures
- Information on how an adversary can defeat the security of your program
- New technology
- Unique applications / capabilities
- Manufacturing techniques / equipment, tools, etc.
- Certain formulas, algorithms, parameters unique to the program or system

CPI Considerations

CPI represents valuable information to an adversary. If an adversary has obtained the program's CPI, they will have key reference points to the critical elements of your program. This exposure could in turn highlight program vulnerabilities, thereby aiding any adversary in the development of potential countermeasures. CPI does not normally apply to system performance characteristics – but rather to those unique characteristics that, if compromised, could kill, counter, afford an adversary the ability to clone the information, or cause a significant alteration to the program. Proprietary information does not always mean CPI, but CPI *could* include proprietary information if it is a unique technology, mission essential application, or technology that will remain only in U.S. systems. CPI is not static and will evolve with the development of the program lifecycle and milestones.

It is important to note that not every program has CPI, but all Acquisition programs must determine if they do or not. CPI is the program's "crown jewels" and is normally few in number. CPI can be either classified or unclassified and is not a repeat of a program's Security Classification Guide (SCG). CPI does not normally apply to unmodified commercial off-the-shelf (COTS) hardware or software, but *could* apply if the program requirements call for a *unique* parameter or software application change to the COTS equipment, which will be incorporated into a U.S. system. CPI can be in any form—information, technology, resources, or the knowledge of a resource.

Appendix A - Critical Program Information Primer

The following questions will assist you in understanding whether or not your program may contain CPI. If your program's information, technology, or resource that is associated with your system's unique capability is lost:

- Could the system be killed or made less effective?
- Could the system be countered?
- Could the system be cloned?
- Would the system have to be significantly modified?
- Would it decrease the system's effective lifetime?

If the answer to any of the five questions above is YES, you probably have CPI and need to consider developing a PPP and associated countermeasures to protect it. If all answers are NO, you may not have CPI inherent to your program. Note: These questions are not *the* determining factor by themselves, but should help give you an indication.

If a PPP is required, it is composed of several parts. There will be basic information about the program and its administration and capabilities, the program's CPI list, general security requirements, a Security Classification Guide, an OPSEC Plan, an Anti-Tamper plan (in most cases), and a Threat Assessment. Each of these areas is coordinated and worked by different specialists. The more specialized areas of the PPP are briefly described below:

OPSEC plan –Operations Security Plan to help protect the program's CPI, Critical Information and other sensitive information and to provide countermeasures to program vulnerabilities based on threat.

Anti-Tamper plan –Provides countermeasures for protecting CPI, other sensitive technologies, and to protect technologies through systems engineering activities intended to prevent or delay exploitation of essential or critical technologies in U.S. systems.

Threat Assessment –Usually composed of a Multi-Discipline Counterintelligence Threat Assessment (MDCITA) performed by NCIS and a full spectrum Threat Assessment coordinated with the Intelligence Community.

Programs that are required to develop a full PPP should start the process well before Milestone B (6-8 months). Depending on program size, development of a PPP can take a several months. For this reason Programs should start the CPI determination process as soon as feasible.

In accordance with the Defense Acquisition Guidebook (formerly DoD 5000.2-R); DoD 5200.1-M; and DoDD 5200.39, if the PM determines that there is no CPI associated with the program (neither integral to the program nor inherited from a supporting program), a full Program Protection Plan (PPP) is not required. In this event, a usually one or two page Abbreviated PPP (APPP) shall be prepared, which will include a statement that CPI does not exist, and the basic process that was used to determine that. The APPP then becomes a document of record and subject to review during milestone decision by the MDA. The APPP will not include the individual parts of a full PPP, although an SCG or general security requirements documents (if program deals with classified information) and or an OPSEC Plan may still be necessary or desired, as determined by the PM. The PPP or APPP must be revalidated at each Milestone after Milestone B.

For programs that are making a determination of whether or not they contain CPI, and assistance with the PPP, the Program Office should notify the SYSCOM RTP representative, who can coordinate the necessary RTP support to the Program.

Appendix B - CPI Validation Tool

NOTE: FORM TO BE COMPLETED BY SYSCOM RTP PERSONNEL

CPI Determination Request Validation Tool

Contact Name:			
Contact Program Office/Program name:			
Phone Number:			
Method Contact initiated: (email/phone/in person)			
Date:		Length of call:	

ASK	Yes	No	Notes
1. Is this now or intended to be a designated Acquisition Program?	Go to 1.a	Go to Option A	Date Acq Prog:
a. Is this a Pre-"MS A" Acquisition Program?	Go to Option B	Go to 1.b	
b. Is there an valid acquisition process requirement (Life cycle)? (MS B, MS C)	Go to question 2.	Go to 1.c	Time to next MS:
c. Has Program submitted or is there an Engineering Change Proposal (ECP), Critical Design Review (CDR) or other significant Program change?	Go to question 2.	Go to 1.d	(e.g. RDC or AAP transition to ACAT compliance)
d. Is there a significant ICD/CDD/CPD change?	Go to question 2.	Go to 1.e	
e. Is this an insertion of new technology?	Go to question 2.	Go to Option E	
2. Is the <u>entire</u> program True COTS (including inherited subcomponents)?	See Option C	Go to Option D	*If Program is completely <u>unmodified</u> COTS then it qualifies ("Yes"). If Program is COTS but modifications are going to be/were made that provided additional or new capabilities, it does not qualify ("No")

Appendix B - CPI Validation Tool

OPTION:	Action:	Comments:
A. Not a valid request for CPI determination	This is not and will not be an Acquisition Program. Advise Program no CPI/PPP requirement for these types of Programs/ Projects. May still be OPSEC, SCG or other security requirements.	
B. CPI Possible, too early in Program development. Not a valid request for CPI determination at this time.	Pre-Acquisition Program (pre CDD/CPD/MS A); Program to contact RTP rep XX months prior to MS B (as appropriate for scale of program).	
C. No CPI	Advise Program no CPI/PPP requirement as Program is entirely a True COTS program. An APPP will be required, and an OPSEC Plan, SCG or other security related documents may still be required.	
D. CPI Possible.	Provide WBS tool. Explain WBS tool, briefly explain establishment of team, and team training.	Time to next MS: "10 Months" Next MS: "MS B" "POPL said it will take them about 3 days to fill in WBS and pick team."
E. Not a valid request for CPI determination	Advise Program no CPI determination or update required if none of the entrance criteria are met. Program to contact RTP rep when one or more of validation criteria are present.	

Appendix C - CPI Data Tracker Tool Metrics Definitions

Meas. Pt.	Phase	Who	Data	How	What do we want to know? How long to make decision?	Calculation	Display (how often)
1	Validate the Request	RTP	Date of Request Date of Decision # Yes, # No Why No? Acquisition Category Time to next Milestone	On the Validation Tool: Transfer to Data Tracker	Ratio of No to Yes Why wasn't it a valid request for CPI determination? ACAT level of program (I, II, III, IV or AAP) Date of next MS for program (how long)	PCT = Date of Decision - Date of initial request Ratio of # no / # yes Categorize the "Why No?" Plot PCT vs ACAT category (Quarterly) Time to next milestones of valid requests vs calendar (Semi-annually)	PCT (days) vs calendar (Monthly) Ratio vs. calendar (monthly) Pareto the Why No? (Quarterly)
2	Set-Up team	POPL	Date WBS Tool Provided Date WBS tool returned to RTP POC	Data Tracker	How long did it take to fill out the WBS and assign POCs? How many times has POPL gone through a CPI ID process?	WBS Tool provided - WBS returned to RTP POC Count Date WBS tool returned to RTP POC - date Team Training Completed End of External Revw - Start of External Revw	PCT (days) vs. calendar (Monthly) Number times through process vs PCT
3	Train the Team		What is POPL's previous experience with identifying/determining CPI? (none, 1-2 times, 3 or more) Size of Team Date Team Training Complete		Number of people on Team How long since team ID to team trained? Cycle Time	Count Date WBS tool returned to RTP POC - date Team Training Completed End of External Revw - Start of External Revw	Size of team vs CPI event PCT (days) vs calendar (Monthly)
4	External Review		Start of External Review End of External Review # People Involved Average Time involved per person # of CPI indicators # WBS line items (total)		Total # of people involved in external review, not just those that completed WBS tool. Touch time How many CPI indicators were found in the external review? How many WBS items were there? Cycle Time	End of External Revw - Start of External Revw Accumulate Touch Time Ratio Ratio CPI Indicators/#WBS lines End date - start date	PCT (days) vs. CPI events (Quarterly) # People vs CPI Events (Quarterly) Cost estimate # CPI indicators vs CPI event Ratio vs. CPI event PCT (days) vs. calendar (Monthly)
5	Internal Review		Start of Internal Review (date) End of Internal Review (Date) # People Involved Average Time involved per person # of CPI indicators No CPI found Start Compile of C-CPI List (Date) Obtain Agreement of C-CPI List (Date) Date CPI list submitted for approval		Total # of people involved in internal review, not just those that completed WBS tool. Touch time How many CPI indicators were found in the external review? How many programs with indicators do not ultimately have CPIs? Cycle Time from start of this phase to agreement on C-CPI. How long for CPI Approval once submitted? What is the first time yield?	Count Accumulate Touch Time Ratio Ratio Agreement Date - Start compile of C-CPI list Date Date CPI list approved - Date CPI list Submitted for approval # yes/ # no over some period or by each PM Categorize the "Why Not?" Estimated Labor Cost = personnel cost phase 4 + personnel cost phase 5 Date CPI list Approved - Date of Request None	# People vs CPI Events (Quarterly) Cost estimate # CPI indicators vs CPI event # No CPI vs # CPI Event Cycle time (CT) vs CPI event Cycle time for CPI Approval vs CPI event Ratio vs Calendar or PM Pareto the Why not Estimated Grand Total Labor Cost vs. CPI Event Cycle time (CT) vs CPI event, CT vs Calendar Quarterly Programs with CPI completing - the upload.
6	List C-CPI		Date CPI list approved Was the CPI list approved the first time? Yes, No and Why Not? Estimated Grand Total Labor Cost CPI ID, Process Cycle Time. Date ASDB update is complete		What was the labor cost of doing CPI determination? What is the Cycle time to identify the CPI? Has the CPI been Uploaded into the ASDB? ASDB is a major tool for Horizontal protection.	Ratio Ratio Agreement Date - Start compile of C-CPI list Date Date CPI list approved - Date CPI list Submitted for approval # yes/ # no over some period or by each PM Categorize the "Why Not?" Estimated Labor Cost = personnel cost phase 4 + personnel cost phase 5 Date CPI list Approved - Date of Request None	Ratio vs. Calendar or PM Pareto the Why not Estimated Grand Total Labor Cost vs. CPI Event Cycle time (CT) vs CPI event, CT vs Calendar Quarterly Programs with CPI completing - the upload.
7	Final List of CPI	RTP					

Appendix C - CPI Data Tracker Tool

CPI Data Tracker Tool

METRICS:

CPI Event Title:		1		2		3		4			5			6		7						
Meas. Pt.	Phase	Validation Of Request		Set-up Team		Train the Team		External Review			Internal Review			List C-CPI		Final List of CPI						
		Valid Request? (Yes, No)	If No, Why Not? Category	ACAT	Time to next Milestone	POPL's previous experience with identifying CPI?	Size of Team	# People Involved	Average Time involved per person (days)	Average Daily cost per person (\$K)	# of CPI indicators	# WBS line items (total)	# People Involved	Average Time involved per person (days)	Average Daily Cost per person (\$K)	# of CPI Indicators	No CPI found? If true enter "0" otherwise leave blank	PM approved first time presented? (Yes, No)	If No, Why Not?	Estimated Grand Total Labor Cost (\$K)		
Data Required	Input Data	RTP Personnel		POPL		POPL		POPL			POPL			POPL		POPL		POPL		RTP		
Meas. Pt.		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Data Required	Request (Date)	Decision (Date)	WBS Tool Provided (Date)	WBS Tool returned to RTP POC (Date)	Team Training Complete (Date)	Start of External Review (Date)	End of External Review (Date)	Start of Internal Review (Date)	End of Internal Review (Date)	Start of C-CPI List (Date)	Compile of C-CPI List (Date)	Obtain Agreement of C-CPI List (Date)	CPI List submitted for Approval (Date)	CPI List Approval (Date)	Cycle time to ID CPI (Days)	CPI Uploaded into ASDB (Date)						
Input Date	RTP Personnel																					
Who	POPL																					

These metrics are intended to be collected from the very beginning to the end of the process. If you need additional information on what is intended or required for a particular metric field, review either the help (comment) pop-ups, or the 'Metric Definition' Tab. There are additionally help pop-ups on some Metric Definition fields. It is best to complete these metrics as the process is completed, rather than at the end.