

Guarding the Crown Jewels

Identifying Critical Program Information

ARION N. "PAT" PATTAKOS

Program managers and other key personnel who make decisions as part of the acquisition management framework are very sensitive to the imperatives associated with cost, schedule, and performance. But the principal consideration when fielding a system should be its performance in the hands of the warfighter. Determining the potential for success in battle emphasizes the notion that opposing forces not have the capability to counter, kill, or reduce the effective combat life of a fielded system.

DoDI 5000.2, Operation of the Defense Acquisition System (May 12, 2003), makes clear in several places that programs with critical technologies/systems must develop plans to protect their "crown jewels," more officially labeled "critical program information" (CPI) during both development and sustainment.

PMs must examine their programs critically to determine if they have CPI. If they do, a program protection plan with an anti-tamper annex is required and must be summarized in the acquisition strategy no later than Milestone B. (If PMs determine that their programs have no CPI, this must be certified in writing to the Milestone Decision Authority.) It is certainly to a PM's advantage to identify CPI as early as possible before Milestone B, given the potentially profound impact that failure to protect CPI might have on schedule, cost, and performance. As a side note, technology protection is a specific inspection item of the DoD inspector general.

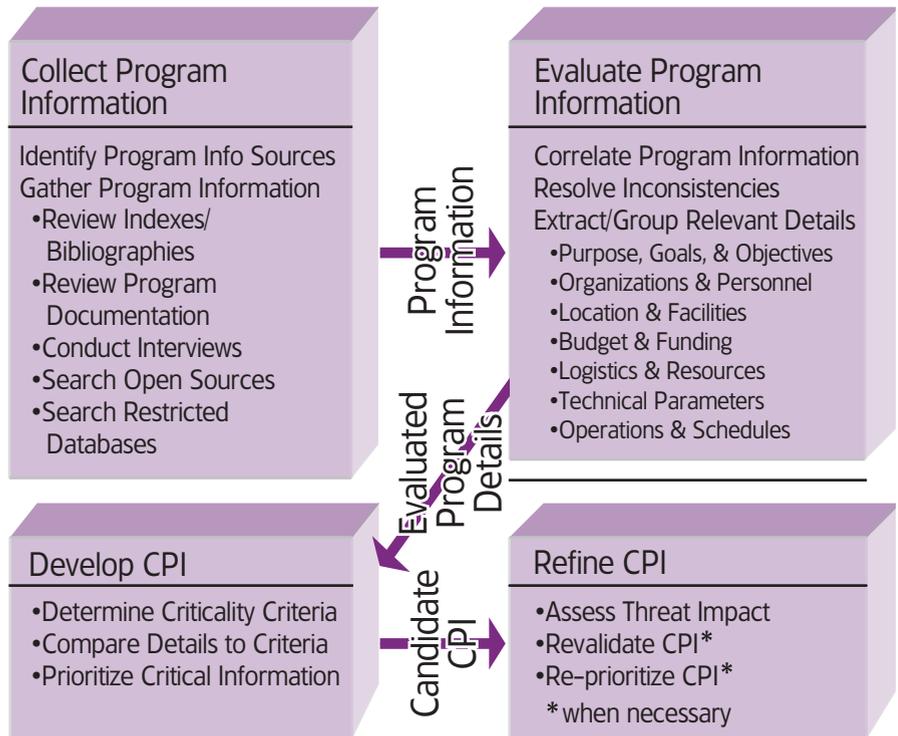


FIGURE 1. The process for Identifying Critical Program Information

Determining CPI

So what are the criteria for determining CPI? Three were mentioned in the first paragraph: the capability of an adversary to counter, kill, or reduce the effective combat life of the system. To that list are added two more. The fourth criterion is "clone"—in other words, sufficient information for an adversary to develop a like system or even skip a generation and develop one that is superior. Obviously not a good situation for our forces to face when deployed. The fifth criterion is the requirement for additional research and development (R&D)—and hence dollars—to achieve the capability required by the warfighter

in the event that it is determined that an adversary has exploited system CPI. Figure 1 gives a graphical view of the overall process for determining CPI.

PMs need to identify and prioritize CPI for any component, subsystem, technology, demonstrator, or even independent research program, the results of which may later be incorporated into their programs. This last may prove difficult, as it raises concerns associated with basic, advanced, and applied research and protecting related information. Most researchers believe—and rightly so—that technology is advanced by openness and retarded by secrecy; however, there exists a gray zone between the two that must be determined if we are to field successful systems (Fig-

Pattakos is the senior advisor to the president/CEO of Beta Analytics International, Inc. He is a certified protection professional (CPP) and an operations security professional (OSP).

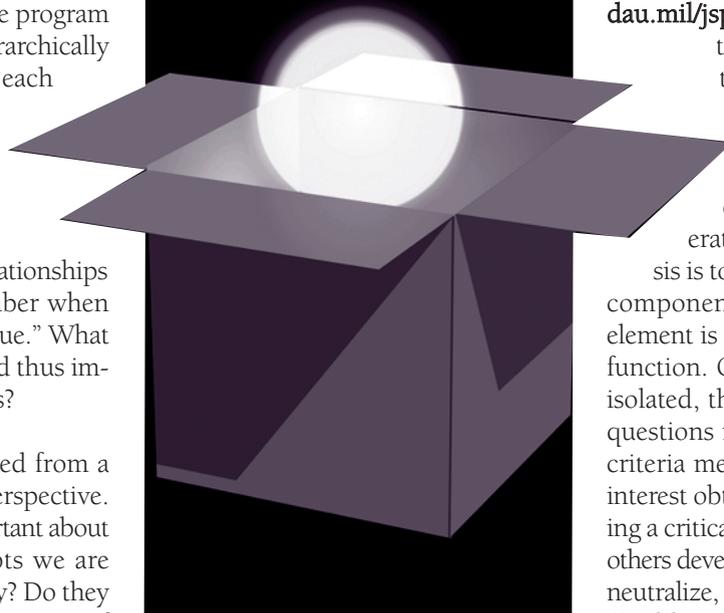
ure 2). It makes sense for the R&D community to ask if a technology is likely to end up in a system used by the warfighter and if that technology is likely to be designated as CPI.

Blue/Red Analysis

A blue/red analytical approach is suggested for the identification of CPI. The blue analysis addresses CPI from a U.S. perspective. What do we think are the key/critical elements of the program (and thus CPI) and why? The analytical process includes performing a "functional decomposition" of the system to isolate what is central to its success. A potentially good beginning in decomposing a system may be found in a review of the Militarily Critical Technologies List (MCTL). The MCTL is the systematic, ongoing assessment and analysis of technologies to determine which are militarily critical. Another source is a well-executed work breakdown structure (WBS). While a PM is not required to have a WBS, the Defense Acquisition University (DAU) advises that it is a derived requirement and a "best practice." Per MIL Handbook 881, the WBS provides the framework for specifying the objective of the program and defines it in terms of hierarchically product-oriented elements, each providing logical summary points for assessing technical accomplishment. One objective of the WBS is to separate component parts to make relationships clear. A key word to remember when doing a CPI analysis is "unique." What makes the system unique and thus important to our military forces?

The red analysis is conducted from a foreign interest/adversary perspective. What do "they" think is important about the technologies or concepts we are using or plan to use, and why? Do they have similar systems in some stage of development? More specifically, the intelligence community should be asked to determine foreign interest targets associated with or relevant to a program. Here too the MCTL is a useful document, since it provides a foreign technology assessment. Another source that

It is certainly to a PM's advantage to identify CPI as early as possible ... given the potentially profound impact that failure to protect CPI might have on schedule, cost, and performance.



program personnel can use to develop questions for the intelligence community is the unclassified version of the annual *Technology Collection Trends in the U.S. Defense Industry* prepared by the Defense Security Service.

The goal of the blue/red analysis is to determine if there are asymmetries in the conclusions. If there are, then these asymmetries require resolution. Why is or is not an adversary targeting relevant technologies? Do they already have the information they need? Why are they targeting something we have not selected as possible CPI? Did we overlook something? Answers to these and related questions will help refine our selections.

Team Approach: the Role of a Security WIPT

Determining CPI is not a one-person effort. A security working integrated product or process team (WIPT) reporting to the PM is recommended to support the entire program protection planning process. The team should include engineers, scientists, users, logisticians, other program personnel, as well as security, counterintelligence (CI), and intelligence personnel all of whom make distinct contributions to the necessary analyses.

A 1999 document supporting technology protection located in the legacy Defense Acquisition Deskbook (accessible at <http://deskbook.dau.mil/jsp/legacy.jsp>) suggests that

the WIPT conduct the functional decomposition by analyzing specific components or attributes that give the system under examination its unique operational capability. This analysis is to be performed on each sub-component until a specific critical element is associated with each system function. Once these components are isolated, the WIPT can ask a series of questions related to the CPI selection criteria mentioned above. If a foreign interest obtained information concerning a critical element: (1) Could they or others develop a method to kill, degrade, neutralize, or clone the U.S. system? (2) Could an advanced method (second generation) be developed that exceeds the first generation capability of the U.S. system? (3) Would the U.S. system need major modification to maintain the strategic or tactical advantage on the battlefield for the system's projected operational lifetime? An answer of "yes" to

any of these questions will qualify the item as a candidate CPI. Other questions require a response: What is the extent to which the CPI could benefit a foreign interest? How difficult is it for a foreign interest to exploit the information?

These questions do not preclude the WIPT's establishing additional criteria. For example, will exploitation of information associated with a critical element permit a foreign interest to seize control of the system? To violate confidentiality, integrity, availability (assured service) considerations? Are there authentication and non-repudiation issues?

The system under development needs to be considered in its total acquisition environment. The WIPT, and thus the PM, must consider the engineering processes, fabrication techniques, diagnostics equipment, simulators, or support equipment for possible CPI. A hard look is required when unique processes are involved to identify any activity unique to the U.S. industrial or technology base that may limit the ability of a foreign interest to reproduce or counter the system. With the decrease in the number of defense contractors, limited sources for the manufacture and production of components for our system may be a consideration.

In the "old days" the term "dual use technology" raised issues of military technologies that were useful for civilian (commercial) applications. Today, it is more likely that technologies developed for the commercial world may have military applications. Thus it is very possible that a system will incorporate unclassified or unclassifiable technologies that nonetheless meet CPI criteria. The quandary is, how do you protect this type of information? After all, if the information can kill, counter, etc., the system, and if foreign interests/adversaries have access to the technology and know that we are using it in our system—we have a problem. A possible approach to solve the dilemma associated with this scenario is to protect the fact of such use in a system. Another possibility is to

It is certainly to a PM's advantage to identify CPI as early as possible ... given the potentially profound impact that failure to protect CPI might have on schedule, cost, and performance.

protect the way we integrate the technology into the system or the fabrication process.

Prioritizing CPI

As one can infer from the previous discussion, all CPI do not carry equal weighting. The analyses supporting responses to the questions noted previously should permit the PM to list CPI in priority order. Such prioritization is necessary to perform an effective security risk assessment based on an analysis of assets (CPI), threats, and vulnerabilities. By assessing risk and establishing the relative order of risk to our CPI, we can better apply protection resources. Here is one of many possible ways to establish a linguistic scale for determining relative CPI priorities:

High/Critical (H/C): Information compromise degrades system combat effectiveness >75 percent or alters significantly program direction to meet mission needs or enables an adversary to copy the system or to skip a generation.

Medium/Critical (M/C): Information compromise degrades system combat effectiveness >50 percent or requires additional RDT&E resources to counter the impact of compromise.

Low/Critical (L/C): Information compromise would degrade system combat effectiveness >25 percent or would

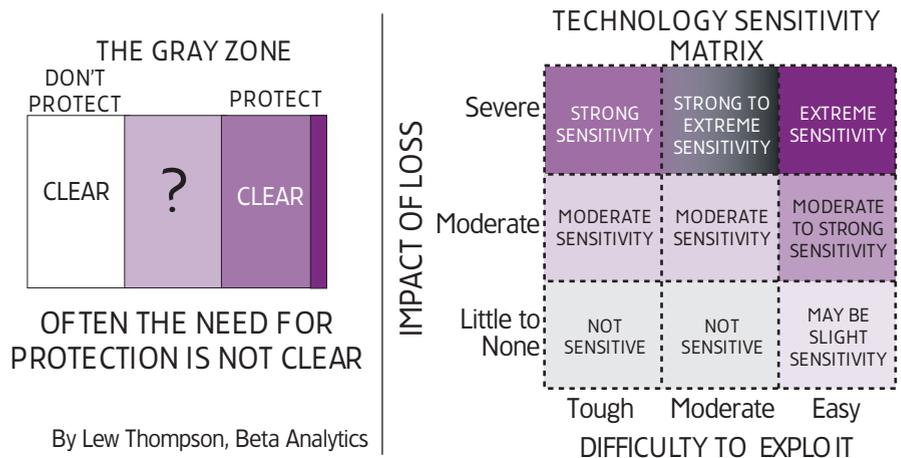


FIGURE 2. The Gray Zone: Identifying When Research Requires Protection

shorten its expected combat-effective life by three or more years.

Horizontal Protection

According to DoD 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection (10 September 1997), CPI must be protected to the same level in one program as in another (called horizontal protection) lest we have a significant exploitable protection weakness. Concerns with the requirement for interoperability further emphasize the need for across-the-board protection. Thus, a common language is needed to identify associated technologies and processes. It is recommended that the MCTL be used as the data dictionary for CPI identification. The MCTL describes technologies critical to maintaining a U.S. military advantage and provides information on the status of those technologies in foreign countries. Unfortunately, no centralized database has been created to match and/or compare research and technology information associated with more than one scientific and technical activity or acquisition program. The CI/security community has planned this—for a number of years—as a future undertaking and is making strides in establishing data elements.

In Conclusion

CPI represents the jewels in the crown of our defense system. Identifying these jewels is a critical first step in a security risk management/program protection planning process. It is key to developing a multi-discipline counterintelligence threat assessment to the CPI and, indeed, to determining its vulnerability to foreign interest collection. As is true of the military commander, the PM is responsible for what his/her program does or fails to do. Fielding a system capable of success in battle is the principal criterion for establishing the success of a PM. Our military forces expect and should receive no less.

Editor's Note: The author welcomes comments and questions about this article. Pattakos can be reached at pattakos@mail.betaanalytics.com.

MCDANIEL APPEARS ON TV, SPEAKS OF THE POWER OF FELLOWSHIP

Judith M. Greig

“A lot of what bothers people—weather, food, clothes, and so on—just isn't significant.” These were the words of Norm McDaniel, associate dean for outreach and performance support, DAU-C/NE, to Dr. Robert H. Schuller, host of the *Hour of Power* TV show, and to viewers nationwide on August 10, 2003. Almost seven years as a prisoner of war during the Viet Nam conflict, suffering torture and deprivation, gave McDaniel a deeper appreciation of what is truly important: having a source of internal strength on which to draw; being able to put one's own situation into the perspective of the cosmic picture; and knowing that one isn't alone, that there is fellowship.

After his introduction to a standing ovation, and before speaking of his own experiences, McDaniel, a much-decorated (see photo caption) retired Air Force colonel with 28 ½ years active duty, recognized his fellow NAM-POWs (Vietnam Prisoners of War) on the 30-year anniversary of their release from captivity under “Operation Homecoming.”

Later he described how he and his fellow POWs had kept each other's spirits up using the “tap code,” a system of communication learned by some of the captive Navy fliers in survival training and soon picked up by the others, including McDaniel, after being imprisoned. The first message he was able to understand was a great source of strength because it was a link with home, McDaniel said. The message identified the prisoner in the next cell as being from North Carolina—McDaniel's own home state.

Tap code communication—indeed, all communication—was covert. If prisoners were discovered, they were punished by torture. Stressing the power of



Norm McDaniel with *Hour of Power* host, Dr. Robert H. Schuller. Among McDaniel's many decorations and awards are the Air Force Silver Star, Defense Superior Service Medal, three Legions of Merit, Purple Heart, Prisoner of War Medal, and Vietnam Service Medal with 14 Bronze Stars.

Photo by Jean Carol (Breeze) McDaniel.

fellowship, McDaniel said, “The enemy knew the strength of prisoners' staying in touch and encouraging each other.”

A strong believer in teamwork and having the right values and view of life, McDaniel encourages everyone he meets to make the most of each day by enjoying the day, helping others, and being thankful for the opportunities and freedoms we have in the United States.

McDaniel's inspiring presentation will be available in text and video formats for a limited time at <<http://www.hourofpower.org>>.

Greig is managing editor of *PM Magazine*, DAU Press, Fort Belvoir, Va.