

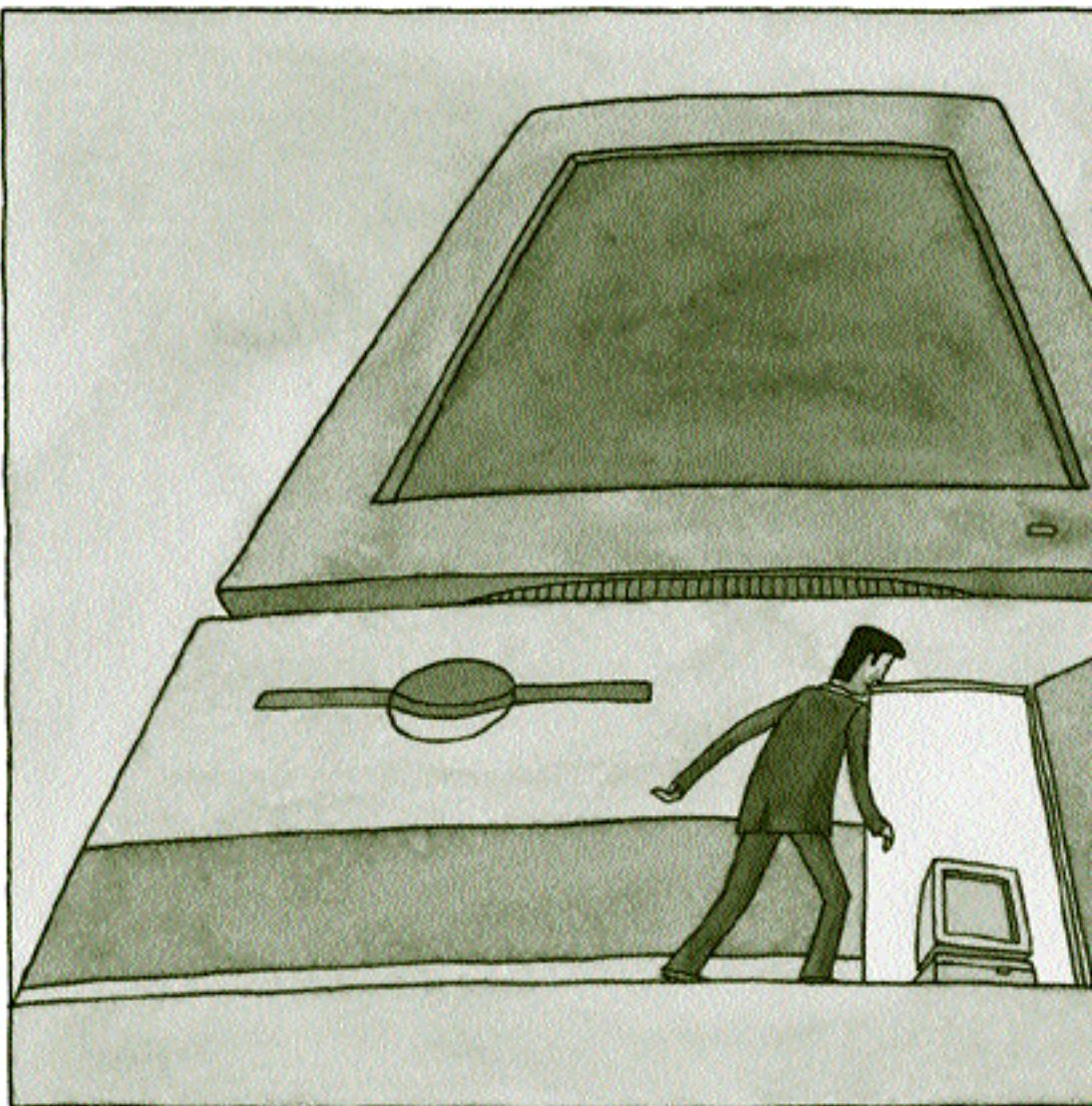
Security Support to Acquisition of Weapons Systems

Vital to Success on the Battlefield

ARION N. "PAT" PATTAKOS

The word *security* is not synonymous to a bad four-letter word. For some it may seem so if it adds further requirements, or seems to impede progress during research and development activities or the formal weapons systems acquisition process. The fact is that security, intelligence, and counterintelligence support to the acquisition of weapons systems is necessary for achieving success on the battlefield.

People in the protection business are not there to impede progress and yes, they are sensitive to the imperatives placed on program personnel dictated by cost, schedule, and performance. They are driven by the mandate to help field systems that have not been compromised, but nevertheless are open to exploitation by those not so friendly to our nation's interests. If you tend to equate security with a bad four-letter word, make it a good one such as *help*—a way to help field successful systems.



Program Protection Plan

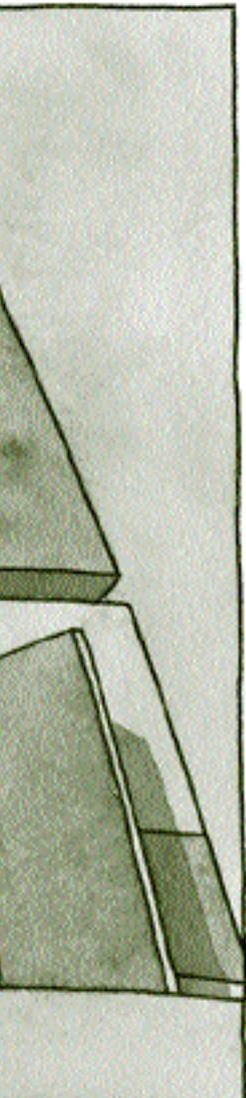
DoD has now rescinded the outdated DoD 5000-series documents, and issued interim guidance pending the development and coordination of policies that are flexible and designed to more rapidly respond to warfighter needs.

Such concepts as evolutionary acquisition and spiral development are now important acquisition strategies, but the essentials of the various phases associated with the Milestone (MS) A through C decision points are the same in the interim guidance.

Concept and Technology Development are based on user needs and technology opportunities. When an affordable, militarily useful capability has been identified and demonstrated in a relevant environment (and can be developed for production in normally less than five

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 (OCP).

years), the System Development and Demonstration Phase is entered with a Milestone B decision. Milestone B is the point at which an acquisition program is initiated. Prior to this decision, the guidance states, is when the identification and protection of Critical Program Information (CPI) must be ensured. It is at Milestone B that a Program Protection Plan (PPP) is required once the CPI is identified (Figure 1).



People in the protection business are driven by the mandate to help field weapons systems that have not been compromised, but nevertheless are open to exploitation by those who would kill the system, counter it, copy it, shorten its expected combat life, or cause a significant redesign of the system and hence expenditure of more research and development dollars.

Protecting CPI

When determining CPI, the term “crown jewels” should come to mind. CPI literally means that information, technology, or systems would cause significant harm if exploited by an entity inimical to our nation's interests. Among the criteria for determining such harm to a weapons system are our adversaries’ abil-

ity to kill it, to counter it, to copy it, to shorten its expected combat life, or to cause a significant redesign of the system and hence expenditure of more research and development dollars.

If adversaries can do one or more of these damaging actions, an acquisition program must take steps to protect the identified CPI. In the case where programs do not have CPI, program managers must so certify in writing to the Milestone Decision Authority (MDA). If CPI does not exist, a PPP is not required.

Scientists, engineers, and other program personnel are schooled in applying various analytical processes to determine and achieve goals. Increasingly, so are Security and Counterintelligence (S/CI) personnel. This community of professionals recognizes that no longer is it acceptable to impose security requirements based strictly on book specifications or regulations. Rather, it is more effective to examine security needs in their specific environments. Just as program personnel are familiar with Risk Management techniques, so too are S/CI professionals.

The analytical process for protecting CPI is embodied in the requirement that program managers or their representatives prepare a PPP (as stated in

Attachment 2 to DoD's 5000-series interim guidance). The PPP is required by MS B (if CPI exists) and thus logically must be prepared during the phases associated with pre-systems acquisition following the Milestone A decision. S/CI personnel counsel that developing the PPP as early as possible during MS A phases will avoid future security prob-

lems that might impact those project-sensitive areas of cost, schedule, and performance. The goal: our fielding of an effective system that is protected and secure from exploitation by the bad guys during combat.

PPP uses a Risk Management approach to identify, recommend, and implement security countermeasures designed to reduce risk to an acceptable level at an acceptable cost. When we use the term acceptable, we mean the person responsible for the system—the one who makes the resource decisions—usually the project manager or, in some cases, the MDA. A PPP describes what must be protected and why, against whom, what vulnerabilities might be exploited, and the necessary countermeasures for protecting the identified CPI.

A key step of the PPP process is the identification of what needs protection—the CPI—and why it needs protection. The “why” question is answered by establishing the adverse impact if an individual CPI is exploited based on the criteria cited (kill, counter, clone, etc). If more than one CPI is identified, metrics can be developed that establish the relative order of CPI importance. Such metrics give a clearer picture of the security risk when viewed in relationship to threat and vulnerability.

You Get What You Ask For

With CPI identification, it logically follows that we then must answer the question: “From whom do we need to protect CPI?” The counterintelligence community is charged with identifying the adversary collection threat to a system. Based on an Intelligence Production Request (IPR), written by the program managers or their representatives, a *Multi-Disciplined Counterintelligence Threat Assessment* (MDCITA) is prepared by Service counterintelligence analysts in coordination with members of the intelligence community. The notion “you get what you ask for” comes to mind here. Specifically, the preparation of the IPR is not a trivial exercise if you want an MDCITA that is a significant input to a well-prepared PPP. A program manager cannot just say, “gimmie threat” and

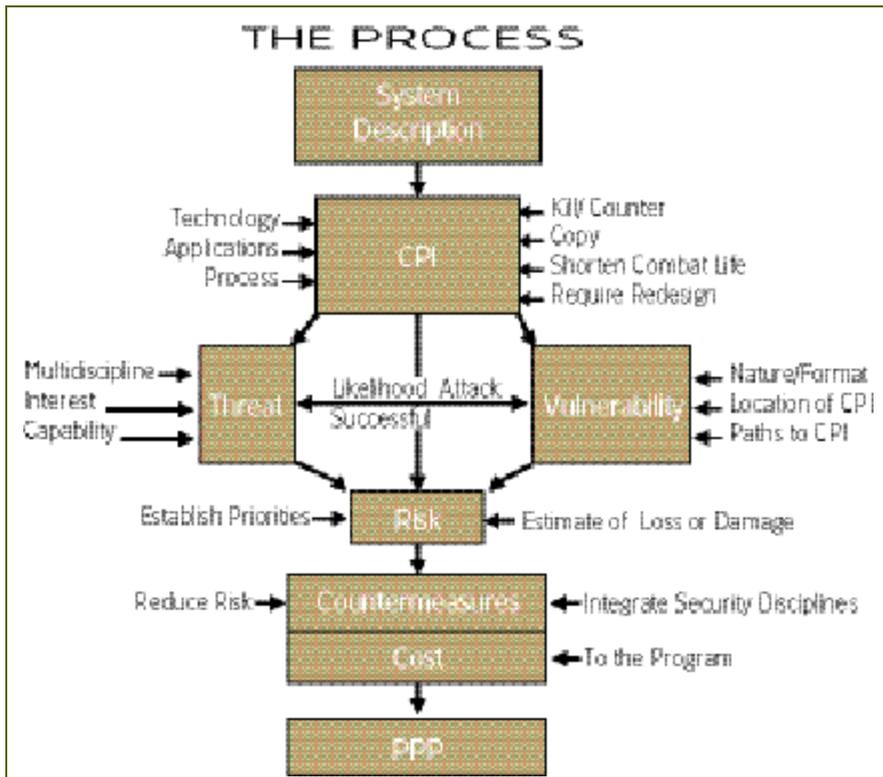


FIGURE 1. Program Protection Planning

expect a helpful response. Supporting S/CI personnel can be of significant help in preparing an effective IPR.

Among other things, a successful IPR requires:

- A clear description of the system and its operational role.
- Details of the CPI and the rationale for its importance.
- The physical location of the CPI and how it exists (its form or format).
- CPI distinguishing traits/emissions and any sight or sensor sensitivities.
- System testing information.
- CPI relationship to key technologies such as those listed in the *Militarily Critical Technologies List*.
- Any anticipated foreign involvement.

A useful MDCITA provides details of adversaries' intent and capability to collect CPI using their human, signals, imagery, and their measurement and signature intelligence capabilities. Essentially, what is sought during this step is an estimate of the likelihood adversaries will target our system and how they might do it. Again, metrics can be developed to describe that likelihood.

An understanding of the threat supports an analysis of how our CPI might be collected by adversaries. This step provides characteristics of weaknesses or potential weaknesses that might be exploited by adversaries. What we seek to understand are those poorly protected pathways that adversaries might use to gain knowledge of our CPI. An exploitable weakness in the protection of CPI is the vulnerability. Some examples of typical vulnerabilities are:

- Lack of need-to-know enforcement
- Failing to use secure communications
- Poor classification management
- Poor computer security/information assurance
- Inadequate visitor controls
- Poor trash management
- Web sites that disclose too much
- Weak security training and awareness.

Metrics can be used to describe the degree of vulnerability.

Risk Reduction

The threat-vulnerability relationship provides an estimate of the likelihood of adversaries' success in accomplishing their target objectives (i.e., collecting

our CPI). The product of the adverse impact to our system (exploitation of CPI), and the threat-vulnerability relationship provides us with an estimate of the potential for loss (the risk) and provides the basis for a risk assessment. A risk assessment is not a mandated element for inclusion as part of a PPP, but is recommended to rank risks in relative order of severity. A risk assessment is the basis for establishing priorities for the effective application of security resources. It also provides a benchmark for determining the benefits of security countermeasures—the reduction of risk (Figure 2).

Security countermeasures are selected to reduce the risk of adversaries collecting and thus potentially exploiting CPI. One definition of the word countermeasure simply is anything that negates adversaries' ability to collect. Countermeasures may include personnel security measures, physical security, procedural measures, and technical security measures. Typical countermeasures include: implementing need-to-know policies; security clearances; implementing security classification guidance; encryption of communications; sound operations security practices; and many, many others.

The principal sections of a PPP include the elements previously described. However, more elements must be considered. These include attaching a time/event-phased security classification guide; a system security engineering management plan; an anti-tamper plan; and if foreign involvement or sales are contemplated, then a technology assessment and control plan is necessary.

While not mandated, developing an Operations Security (OPSEC) Plan is recommended. OPSEC deals with the generally unclassified evidence of sensitive activities or operations. In a message dated Jan. 14, 2003, the Secretary of Defense reminded all that the DoD has more than 700 gigabytes of Web-based data subject to adversary exploitation, and that by using the OPSEC process we could eliminate potential vulnerabilities from that source. Given the

amount of easily available information, determining the information (indicators) that may reveal CPI is critical.

The Counterintelligence community is dedicated to providing the support needed by the research, technology, and acquisition communities. To that end, DoD has designated 450 CI positions (150 per Service) specifically for such support. A Department of Defense Counterintelligence Field Activity (CIFA) has been established that has elements and organizations that support research, technology, and weapons system development. The Joint Counterintelligence Training Academy (part of CIFA) provides a two-week research and technology protection course with such related subjects as Risk Management and PPP.

Policy requires that a Counterintelligence Support Plan (CISP) should be prepared for each Research, Development, Test and Evaluation facility, for those acquisition programs with CPI, and may be extended to those contractor or academic institutions with CPI. The CISP is viewed as a contract between a CI supporting element and the organization supported. The CI representative, the supported element security manager, and the commander/program manager signs the CISP at the local level. Headquarters-level approvals are also necessary. The CISP outlines how 36 support activities, from threat briefings and debriefings to CI support to defensive information operations, will be conducted. The CI commitment to support program managers, commanders, and the entire research and technology community clearly is there.

Tug of War

A subject that has received much attention is when to classify and hence protect technology. S/CI professionals would like to see critical technologies (potential CPI) identified as early as possible during the MS A to MS B phases. Pre-milestone A would be great, some opine. However, the tug of war between enabling basic research and protecting the technologies that will be (or are) key to our systems is understood.

The Security and Counterintelligence (S/CI) community of professionals recognizes that no longer is it acceptable to impose security requirements based strictly on book specifications or regulations. Rather, it is more effective to examine security needs in their specific environments.

National Security Decision Directive 189 and Executive Order 12958 mandate that basic scientific research not clearly related to the national security may not be classified. Our technical know-how

is advanced with the open development and acquisition of knowledge inherent in basic research. But, it appears reasonable to accept the notion that protection is required when the “how” of applying that knowledge to a weapons system is determined. In DoD funding terms, this point lies somewhere between 6.1 (Basic Research) and 6.3 (Applied Research).

Security—A Profit Center

Security should be viewed as a profit center or at least as value added. We profit by fielding systems that support the warfighter if the systems are available when and where needed. Our adversaries' ability to kill, to counter, to clone a system, or to shorten its useful effective combat life does decrease a system's value and the way we profit. Such adverse impacts, in fact, expend resources in terms of lives and money. S/CI personnel, in coordination and cooperation with program personnel, are dedicated to making security work by taking appropriate security and counterintelligence actions at the right time.

The crest of the 902d Military Intelligence Group states: *Strength Through Vigilance*. It does indeed make good common sense.

Editor's Note: The author welcomes questions or comments on this article. Contact Pattakos at Pattakos@betaanalytics.com.

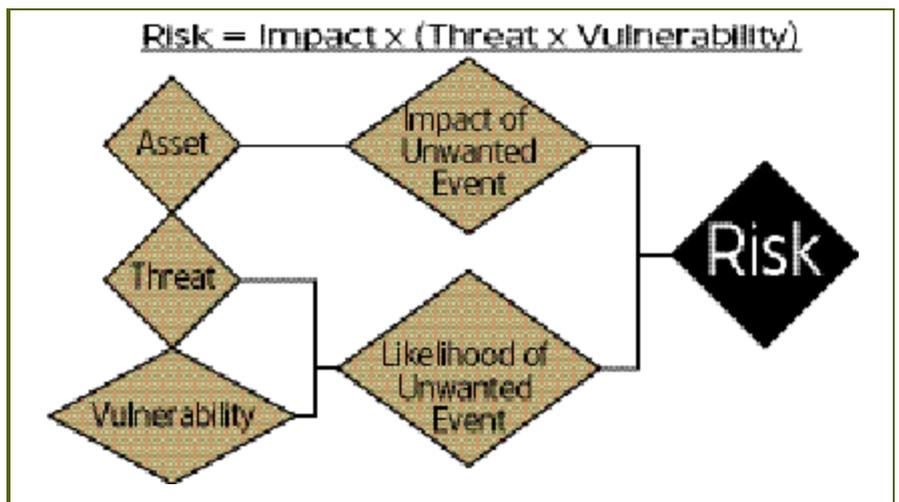


FIGURE 2. Risk Formula