

Position Paper

**Why Are Security Requirements
Not Included
in the Engineering Life Cycle Process?**

Author: Carole Snyder
System Security Engineering
ITT, Systems Division
SpaceLift Range Systems Contract

Phone (321) 494-5374
FAX (321) 494-5338
Email Carole.Snyder@rc.patrick.af.mil

Why Are Security Requirements Not Included (or not included very well) in the Engineering Life Cycle Process?

This document discusses issues concerning the inclusion of security requirements in system design, development and acquisition phases of the engineering life cycle process. Whether a secure product is being built or modified for eventual evaluation and sale, or whether a system is being built or modified for an organization's own use, it must have a set of rational, cost-effective, measurable security requirements. This document describes the use of several DoD regulations and standards that discuss and promulgate computer security requirements. It also discusses the roles and responsibilities of key players (especially the certifier) in the system certification and accreditation process who should ensure that security is included in the engineering life cycle process.

There is a generic engineering life cycle process that is recognized by IEEE, and a similar version is recognized by the DoD. In general, the life cycle process starts with mission needs determination, or system definition, and progresses through many phases, such as preliminary and detailed design, fabrication, assembly, integration and test, and operational support.

Most organizations' projects are not for the development of a complete, new system. Most projects are to upgrade, modify or replace existing systems. Therefore, the entire system development process is tailored to the project and may not require progression through each successive phase of the life cycle process. Some phases may be skipped or combined on smaller projects. Milestones and document requirements are determined in the process of developing the project plan. The milestones and document requirements vary depending on the project objectives. However, when tailoring the life cycle for a specific project, the product or system that is modified or produced must meet specific system requirements. Security requirements are included in those requirements. For organizations (e.g., system or software vendors) that develop secure products for eventual evaluation and sales, the same thing applies; the specific system requirements, including security requirements, must be addressed in the engineering life cycle process.

The DoD 5200.28-Std, "DoD Trusted Computer System Evaluation Criteria", (the orange book) presented evaluation criteria that were easily understood by the vendor community and by the using community (i.e., those who operate and maintain computer systems). It introduced and promulgated computer security terms and descriptions of security features and levels of trust that have been widely accepted and used. Names of security features such as DAC, I&A, and audit are well known throughout the computer security

community. The orange book was aimed at encouraging vendors to create a supply of systems containing security features (i.e., trusted systems).

For the past fourteen years, until it was recently superseded, DoD Directive 5200.28 "Security Requirements for Automated Information Systems (AISs)" was applicable to all components of the DoD and pertained to AISs that handle classified, sensitive unclassified or unclassified information. It stated in its Policy section that security policy shall be considered throughout the life cycle of a system. It further stated that the system developer is responsible for ensuring the early and continuous involvement of the users, system security officers, data owners, and the DAA in defining and implementing security requirements. One purpose of the Directive was to require a more accurate specification of overall security requirements. Another purpose was to promote the use of cost-effective, computer-based security features.

The DoD Directive was aimed at creating a demand for secure systems by stating that mandatory statements of safeguard requirements shall be included, as applicable, in the acquisition and procurement specifications for systems. The Directive presented a set of mandatory minimum requirements that applied to a system that processes classified or sensitive information. The Directive required that a system analysis be done to identify any additional requirements over and above the set of minimum requirements. Those additional requirements mapped directly to the C2 and above levels of criteria in the orange book.

DoD Directive 5200.28 was recently superseded by DoD Directive 8500.1, "Information Assurance (IA)". This directive puts more emphasis on the life cycle approach. The first item in the Policy section states "Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems". Also, this new Directive discusses security solutions that go beyond trusted operating systems, such as firewalls, encryptors, security-enabled web browsers and screening routers. The Directive specifies that the DITSCAP process must be used.

I have some concerns regarding how security requirements are presented in DoD Directive 8500.1. I also have concerns with how this Directive and DITSCAP are supposed to mesh with each other when their terminology is different and their determination of levels of security and identification of requirements are different. The Directive focuses on determining which of several mission assurance categories a system falls into and directs that protective measures be applied according to "commercial best practices", "beyond best practices", and "most stringent". There does not appear to be a defined process for determining the protective measures. The Directive does not specify who makes the determinations and selections of protective measures and does not discuss how these activities merge with the DITSCAP process.

The conference for which this paper was written was intended to focus on the application of engineering principles to system security design. However, I think the bigger issue is why are security requirements not included (or not included very well) in the system life cycle process? System design is a phase of the life cycle process.

For fourteen years, the security requirements were clearly spelled-out in the DoD Directive 5200.28. Has 5200.28 been effective in ensuring that security requirements are identified and included throughout system life cycles?

I think that the effectiveness of 5200.28 has depended on two things:

1. Correct implementing regulations within each of the DoD components.
A component may put their own spin or their own interpretation of 5200.28 in their implementing regulation. But if they are not careful, an erroneous or confusing statement can be extremely costly to those who must implement their regulation. Even 'tweaking up' the level of security, although well-intentioned, can be costly. As an example, requiring all systems to have anti-virus software sounds like a good idea, but, even if doable, it may not be rational for every system in every operating environment. Many "good idea requirements" can result in costly delays, debates, and confusion and may result in installing an inappropriate security solution.
2. Enforcement of the implementing regulations by the component Designated Approving Authorities (DAAs).

Without management support, regulations do not get implemented, or they get implemented incorrectly. For a computer security regulation to be implemented, it takes support from the DAA. Furthermore, the DAA must have a technical computer security expert in the role of the Certifier. The certifier plays a key role in the system certification and accreditation process and must be adept in identifying rational, cost-effective, doable, and testable security requirements that are suitable for a particular system. Mistakes in this area will be costly.

Rational, cost-effective, doable, and testable security requirements do not magically appear in system specification documents and engineers do not search for them and voluntarily include them. Engineers are concerned with the functional and performance specifications and often consider security requirements to be constraints that can be addressed during the installation phase. Technical computer security professionals (i.e., certifiers) need to ensure that security is addressed throughout the system life cycle. A computer security program must be set up and roles and responsibilities must be established before security requirements will be included with the functional and performance requirements.

A few years ago, DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)" was published. The C&A process is not a new process. There was a FIPS PUB in the 70's that described a comprehensive C&A process. But, it only gave brief mention of security in the design and development phases of the life cycle. Back then, the idea of building standardized security features into operating systems was practically unheard of. Furthermore, the security requirements could be met by administrative and procedural means. Even identification and authentication could be done on small systems by using a paper sign-in log. Most mainframes did not have remote users. So there was no real incentive to add security requirements into the design and development phases. Security controls could be retro-fitted in a later phase.

Today's computers are far more vulnerable to unauthorized access. Nearly every process we can think of is computerized. Systems are connected for seamless interfacing of many processes. So, the need to have rational, measurable, cost-effective security requirements included in the life cycle process is greater than ever.

The DITSCAP process, which is to be implemented by all DoD Components, requires the assignment of specific roles and responsibilities of several key players. The key players in the C&A process are the DAA, the program or project manager, the certifier, and the user. The process requires that they be involved in the engineering life cycle to ensure that security is included in the design and development or acquisition of systems. A shortcoming of the DoD Directive 5200.28, and of its replacement, DoD Directive 8500.1, is that they do not address the role and responsibilities of the certifier.

Of the key players, I believe the certifier is the most important player, as he or she is the only player who is presumed to have technical computer security expertise. Unfortunately, the DITSCAP does not emphasize that the certifier be an expert. The DAA needs to be able to rely on the certifier's determination of the adequacy and sufficiency of the security requirements and their implementation and successful testing. The DAA is ultimately responsible for the secure operation of a system and bases the accreditation on the recommendation of the certifier. The certifier's job must not be a desk job nor a part-time assignment. The certifier needs to get to know the existing systems; not how to operate them, but be able to observe the operational environments and have enough technical expertise to comprehend how information is transferred, stored, and shared. The certifier must be involved in new projects as a team member to identify the security requirements and to verify and validate that the requirements are met.

One other possible tool that may help to ensure that security requirements are included in the engineering process is the ISO 9001:2000 Standard. In product development, there are many references to product requirements.

We are in the 3rd year of a large, 10-year contract to upgrade, modernize, sustain, and replace computer systems that support the space launch program. We are committed to the requirements contained in the ISO 9001:2000 Standard and we follow the processes. This is especially important in the engineering life cycle. Hardware and software is designed, fabricated, assembled, and tested under a quality system. My job is to ensure that security is considered in the design, development, sustainment and modification of the computing components of the launch support systems. My security engineering function is part of Specialty Engineering, which also covers reliability, maintainability, and human factors engineering.

Each of our projects has an assigned team consisting of a lead engineer and hardware and software leads (as required). There are team members assigned to represent quality, configuration management, systems security, reliability, depot, shops, and testing, to name a few.

Paragraph 7.1 of the ISO Standard is Planning and Product Realization. It says that in planning product realization the organization shall determine the requirements for the product. The organization shall determine the required verification, validation, monitoring, inspection and test activities specific to the product and to the criteria for product acceptance.

Paragraph 7.2 is Customer-related processes. It says the organization shall determine the requirements specified by the customer. Also the statutory and regulatory requirements related to the product and any additional requirements determined by the organization.

Specific computer security “shalls” are included in our contract documentation. These “shalls” are inserted into system specification documents as applicable. A requirements traceability matrix is developed to ensure that all of the requirements for the project, including the security requirements, can be traced from their origin through design, development and testing to the final product.

Paragraph 7.3 specifically addresses design and development. It says the organization shall determine the design and development stages and the review, verification and validation appropriate for each stage, and the responsibilities and authorities for each stage. The design and development inputs are the requirements. The design and development outputs must meet the inputs. Periodic reviews of design and development stages will include representatives of functions (e.g., systems security). Records of reviews and actions taken shall be maintained.

If the ISO Standard is adhered to, there is assurance of a quality product and a satisfied customer. Compliance with the Standard will ensure that security

requirements are included in the engineering life cycle. In my opinion, vendors who build secure products (e.g., firewalls) should be required to use the ISO Standard for their processes. Also, I suggest that vendors of secure products make available a document that describes the requirements that trace to their product's features and capabilities. Vendor product information is often not specific enough to aid in the decision of whether the product will meet an organization's security needs.

Regarding the question: Why are security requirements not included in the engineering life cycle process? For the DoD Components and other government agencies, there is no excuse. It has been mandated for many years. I can only guess that the computer security program has not been implemented properly at the Component and Agency levels and below. DAAs have been assigned, but they do not have, nor do they need, the computer security expertise to identify the requirements. Program managers do not have the incentive to add security requirements into their projects because they assume (whether it's justified or not) that the security requirements may increase the cost or constrain the design.

Not enough importance has been placed on the fact that the certifier is the "eyes and ears" of the DAA, and is the person who can keep the DAA out of trouble. A certifier who lacks technical expertise and authority can cause costly delays at project completion if the system is ready to be operational, but the adequacy and sufficiency of the security controls are in question and the DAA hesitates from accepting the system. In many DoD component organizations, certifiers with technical computer security expertise have not been hired.

One organization that has successfully implemented effective DAA and certifier roles and responsibilities is the Industrial Security division of Defense Security Service. I believe that they are an exception because they focus on certifications and accreditations as a major function of their organization. The Industrial Security division is responsible for certifying and accrediting computer systems that handle DoD classified information and are operated in DoD contractor facilities throughout the world.

I have not heard of a conference being held for certifiers, and that is probably because there are not enough technical computer security professionals fulfilling certifier roles to warrant a conference for certifiers. Yet, it is ultimately up to the certifier to identify the requirements and ensure that they are addressed throughout the system life cycle process.