Information Assurance
Forethought versus Afterthought

Richard L. Peters
Northrop Grumman Information Technology
Orlando, Florida
rpeters@ideorlando.org

Christian M. Schleipfer
Northrop Grumman Information Technology
Orlando, Florida
chris.schleipfer@ngc.com

ABSTRACT

Starting in late 2002, the Department of Defense (DoD) and the U.S. Army issued major regulatory guidance changes regarding Information Assurance (IA), which have a major impact on the acquisition of automated information systems (AIS) procured by the Department of Defense and its components. The paper will present the new regulatory guidance as it pertains to the certification and accreditation (C&A) of U.S. Army automated information systems. The terms "certification" and "accreditation" will be defined as they pertain to fielding an accredited AIS.

The paper will present the current methodology of incorporating IA into AIS acquisitions to include the lack of IA requirements in RFPs and resulting contracts, the "add-on" or "bolt-on" approach to IA, and the cost and schedule impacts caused by this methodology.

The paper will present a methodology to integrate IA into the AIS acquisition process from the beginning. Included in this methodology is the concept of defining the IA requirements in the RFP to preclude baseline or engineering change requirements after contract award to add security to the program as an afterthought, which is a major cost and schedule driver. The paper will also present the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) compared to the normal acquisition cycle process to depict how the two processes are related and how IA applied as an afterthought or as a forethought affects the two processes.

In summary, the paper will contrast the two methodologies of incorporating IA into AIS acquisitions. Additionally, the benefits of pursuing the new methodology of integrating IA into AIS acquisitions versus the current "add-on" approach will be presented.

ABOUT THE AUTHORS

Richard L. Peters retired in 1991 from the US Army after 26 years of service, the last three of which were as a Project Director within STRICOM. He has been a Program Manager for many information systems development teams, including the resource repository for JSIMS. In 2001, Mr. Peters changed his job focus to Information Security. He successfully supported the certification and accreditation of the Mobile Automated Instrumentation System (MAIS) and is currently leading the effort to certify and accredit the Common Training Instrumentation System (CTIA) and the National Training Center Objective Instrumentation System (NTC-OIS). Mr. Peters achieved certification as an Information System Security Professional (CISSP) in March 2004.

Christian M. Schleipfer has numerous years of experience in the areas of Networking and Telecommunications, including access control and closed circuit television. This work was in the commercial sector for Circuit City. He served as the configuration manager for the Mobile Automated Instrumentation System (MAIS), prior to changing his focus to Information Security. He is currently heading the effort to certify and accredit the Digital Multipurpose Range Complex (DMPRC) for Ft. Hood, TX. He has been nominated to head the effort to certify and accredit the Digital Range Training System in 2004. Mr. Schleipfer achieved certification as an Information System Security Professional (CISSP) in March 2004.

Information Assurance
Forethought versus Afterthought

Richard L. Peters
Northrop Grumman Information Technology
Orlando, Florida
rpeters@ideorlando.org

Christian M. Schleipfer
Northrop Grumman Information Technology
Orlando, Florida
chris.schleipfer@ngc.com

INTRODUCTION

Information Assurance (IA) within the Department of Defense (DoD) is a complex domain, which has its own set of regulatory guidance, policy, procedures, and acronyms. Since late 2002, IA has evolved from the Trusted Computer Security Evaluation Criteria (TCSEC) methodology to a defense-in-depth methodology. To understand this evolution, a person must be familiar with latest regulatory changes over the past two years. In the past and currently, IA, previously known as Information System Security, has been an add-on to information systems after contract award, i.e., an afterthought, which increases the cost and lengthens the schedule for information system procurement. If IA is implemented as a forethought, i.e., prior to contract award, the cost of IA will be lower and the system schedule should not be impacted.

This paper is Army system centric; however, it is applicable to all automated information systems (AIS) procured by the Department of Defense. This paper is not applicable to information systems that process intelligence, sensitive compartmented, or higher information, because they are accredited under a different set of regulatory guidance.

IA REGULATORY GUIDANCE EVOLUTION

The Beginning of IA Change within DoD

The evolution of IA regulatory guidance from the Trusted Computer Security Evaluation Criteria methodology to a defense-in-depth methodology began with the publication of Department of Defense Directive (DoDD) 8500.1, *Information Assurance (IA)* on October 24, 2002. DoDD 8500.1 superseded the following publications:

a. DoD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988
b. DoD 5200.28-M, *ADP Security Manual*, January 1973
c. DoD 5200.28-STD, *DoD Trusted Computer Security Evaluation Criteria*, December 1985
d. DoD CIO Memorandum 6-8510, *Guidance and Policy for Department of Defense Global Information Grid Information Assurance*, June 16, 2000

DoDD 8500.1 is applicable to all DoD owned or controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity. It did not alter or supersede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333. DoDD 8500.1 does not apply to weapons systems as defined by DoDD 5137.1, *Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)*), February 12, 1992.

DoDD 8500.1 states that requirements for availability and integrity are associated with the mission assurance category of the system, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know of the information processed by the system. Both sets of requirements are primarily expressed in the form of IA controls, which were not defined in DoDD 8500.1; however they are fully defined in its implementation instruction published in February 2003.

Impact of DoDD 8500.1

DoDD 8500.1, by itself, did not have a major impact in terms of IA requirements to be met in order to achieve certification and accreditation (C&A). However, it changed the underpinnings upon which certification and accreditation are based from the Trusted Computer Security Evaluation Criteria methodology to a defense-in-depth approach.

Implementation of IA Change within DoD

DoD Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation*, was published on February 6, 2003 and implemented the policy, assigned responsibilities, and prescribed procedures for applying integrated, layered protection of the DoD information systems and networks in accordance with (IAW) DoDD 8500.1. The major impact of DoDI 8500.2 is the establishment of a baseline level of information assurance for all DoD information systems through the assignment of IA controls to each system. Assignment of IA controls is made according to the mission assurance category of the system and the confidentiality level of the information the system processes. Before going further into IA controls, it is necessary to define the terms and levels of mission assurance category and confidentiality.

Definition and Levels of Mission Assurance Category

Mission Assurance Category (MAC) reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The DoD has three defined mission assurance categories:

a. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures and require high integrity and availability controls.

b. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance and require high integrity and medium availability controls.

c. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices and require basic integrity and availability controls.

Definition and Levels of Confidentiality

The confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The DoD has three defined confidentiality levels: classified, sensitive, and public.

a. Classified Information. Information that has been determined pursuant to Executive Order 12958 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

b. Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552A of Title 5, United States Code, *The Privacy Act*, but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of Title 15, United States Code, *The Computer Security Act of 1987*). This includes information in routine DoD payroll, finance, logistics, and personnel management systems.

c. Public Information. Official DoD information that has been reviewed and approved for public release by the information owner in accordance with DoDD 5230.9, *Security and*

Policy Review of DoD Information for Public Release, August 6, 1999.

IA Controls

An IA Control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and activities required to achieve the IA Control are assignable and thus accountable. A specific set of IA Controls is applicable to each mission assurance category and each confidentiality level. Each IA Control may have one, two, or three levels (1 – 3). The levels generally align to the mission assurance category or confidentiality levels; however, there are exceptions. Table 1. IA Controls by Mission Assurance Category and Confidentiality Level shows the number of IA Controls for availability and integrity associated with each MAC level and the number of IA Controls for confidentiality associated with each confidentiality level.

Table 1. IA Controls by Mission Assurance Category and Confidentiality Level

MAC or Confidentiality Level	Number of IA Controls
MAC Level	
MAC I	Availability & Integrity: 70
MAC II	Availability & Integrity: 70
MAC III	Availability & Integrity: 64
Confidentiality Level	
Classified	Confidentiality: 45
Sensitive	Confidentiality: 34
Public	Confidentiality: 10

The IA Controls for mission assurance category and confidentiality levels are independent, i.e., a MAC I system may process public information and a MAC III system may process classified information. This means that there are nine combinations of mission assurance category and confidentiality level IA Controls, which establish the nine baseline levels that may coexist within the Global Information Grid (GIG). The set of IA Controls applicable to any given DoD information system is always a combination of the IA Controls for its mission assurance category and the IA controls for its confidentiality level. Table 2. IA Controls by Combination of MAC and Confidentiality Level shows the total number of IA Controls for each combination of MAC and confidentiality level.

Impact of DoDI 8500.2

Unlike DoDD 8500.1, DoDI 8500.2 did have a major impact in terms of IA requirements to be met in order to achieve certification and accreditation. As shown in Table 2, the number of IA Controls that must be met is dependent upon the combination of mission assurance category and confidentiality level IA Controls. DoDI 8500.2 increased the number of security requirements to be met for certification and accreditation by a factor of two to three over previous regulatory guidance. These increases impact both cost and schedule for the system being accredited. On the plus side, DoDI 8500.2 did standardize the security requirements necessary to achieve accreditation.

Table 2. IA Controls by Combination of MAC and Confidentiality Level

MAC and Confidentiality Combinations	Total Number of IA Controls
MAC I, Classified	115
MAC I, Sensitive	104
MAC I, Public	80
MAC II, Classified	115
MAC II, Sensitive	104
MAC II, Public	80
MAC III, Classified	109
MAC III, Sensitive	98
MAC III, Public	74

Implementation of IA Change within the Army

The U.S. Army brought its IA regulatory guidance in line with the DoD IA publications with the release of Army Regulation (AR) 25-2, *Information Assurance* on November 14, 2003. AR 25-2 superseded the following publications:

a. AR 380-19, *Information Systems Security*, February 27, 1998.

b. HQDA Letter 25-02-1, *U.S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy*, April 15, 2002.

c. HQDA Letter 25-03-1, *Transition of Information Duties and Responsibilities*, April 23, 2003.

Summary of Changes

AR 25-2 implements the concepts of defense-in-depth, mission assurance category, and levels of confidentiality within the Army, which were introduced and described in DoDD 8500.1. The

regulation introduces the concept of IA Best Business Practices to facilitate the Army's ability to adapt to changing technology or implementation guidance. AR 25-2 adds and defines an IA personnel hierarchy and changes the titles of IA personnel from Information Systems Security to Information Assurance. The regulation outlines monitoring guidelines and requirements for Army networks. AR 25-2 also adds requirements for a Communications Security Logistics Activity to provide an Army cryptographic applications certification process and involvement in the life-cycle management of information systems. AR 25-2 states that MACOMs, PEOs, PMs, or functional proponents will not field, and installation commanders will not accept:

a. Systems that do not meet minimum security standards stated in the acquisition and procurement specifications.
b. Systems for which the DOD or Army DAA does not provide complete documentation supporting C&A.
c. Systems that have not undergone certification testing and received appropriate accreditation.

Punitive In Nature

Violations of several of the paragraphs within AR 25-2 may be punished as violations of a lawful general order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or contractual actions as applicable. The cited paragraphs within the regulation and other provisions of the regulation might be the basis for a commissioned, warrant, or noncommissioned officer to issue a lawful order to a solider. Penalties for violations of the above-cited provisions of the regulation, and orders based on these and other provisions of the regulation, include the full range of statutory and regulatory sanctions. Personnel not subject to the UCMJ who fail to comply with these requirements are subject to disciplinary, administrative, or prosecutorial actions as authorized from criminal or civil sanctions under sections including, but not limited to, the United States Code, contractual support obligations, or Federal or state regulations.

Impact of AR 25-2

AR 25-2 supplemented the IA Controls defined in DoDI 8500.2 and added additional security requirements that must be met to achieve certification and accreditation of Army systems. Its major impact on the Army community is the punitive nature of the regulation. AR 25-2 also states that systems will not be fielded, nor accepted for fielding if they are not accredited.

IA Change in the Near Future

An informal coordination draft of DoDI 8510.bb, *DoD Information Assurance Certification and Accreditation Process (DIACAP)* was released for review on March 19, 2004. This publication, when approved, will supersede the following publications:

a. DoDI 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP),* December 30, 1997.
b. DoD 8510.1-M, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual,* July 2000.

DoDI 8510.bb establishes the standard DoD process for identifying, implementing, and validating IA Controls, for authorizing the operation of DoD information systems, and for managing IA posture across DoD information systems consistent with the *Federal Information Security Reform Act of 2002* (FISMA) and DoDD 8500.1. DoDI 8510.bb also authorizes the publication of DoD 8510.bb-M, which has been released as a draft annotated outline on March 19, 2004.

Impact of DoDI 8510.bb

DoDI 8510.bb will replace DoDI 5200.40, known as the DITSCAP, as the process to certifying and accrediting DoD systems. It is meant to reduce the amount of documentation required to achieve accreditation. DoD 8510.bb-M will be a replacement for DoD 8510.1-M and will provide the details of implementing the DIACAP described in DoDI 8510.bb.

Certification and Accreditation

Certification

Certification is the comprehensive evaluation of the technical and non-technical security features of an information system (IS) and other safeguards, made in support of the accreditation process. Certification establishes the extent to which a particular design and implementation meets a set of specified security requirements. The Certification Authority (CA) is the individual responsible for making a technical judgment of the system's compliance with stated requirements by identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Accreditation
Accreditation is the official authorization to field an IS and is based, in part, on the formal certification of the degree to which a system meets a prescribed set of security requirements. Accreditation must address each operational environment of the IS for both fixed and deployable configurations. The Designated Approving Authority (DAA) is the official with the authority to formally assume responsibility for operating an IS or network at an acceptable level of risk.

IA AS AN AFTERTHOUGHT

In the past, and for many of the current automated information systems being fielded, IA has been an add-on to the system after the contract has been awarded, i.e., an afterthought. When IA is an afterthought to an automated information system procurement, the usual result is an increase in cost and schedule during either the design, development, or procurement phase. Figure 1 depicts the process discussed in this section with the DITSCAP shown under the normal acquisition cycle process

Past and Current Process

The process described in this section is generally applicable to automated information systems that process secret or below information, which do not contain compartmented information. Information systems that process top secret, compartmented, or higher information are not considered because those systems have a different regulatory process, and tend to conduct certification and accreditation in a much more proactive manner than secret or below information systems.

Prior to Contract Award
After an operational requirements document is approved for an information system, the government procurement team develops a request for proposal (RFP), which may or may not contain a product specification. During RFP development, IA is either not considered at all, or not considered in any detail. A contributing factor to the lack of IA input into the RFP is that the IA staff, within the procurement organization, is usually not involved as part of the RFP development team, or the RFP review process prior to the RFP release. Because the IA staff has little or no involvement in the RFP development, the RFP development team has limited knowledge of the IA process and proceeds with a business as usual approach to the procurement, with minor consideration given to IA. The result of this limited understanding of the IA process and conducting business as usual is normally the inclusion of one or more of the following requirements in the RFP or product specification:

a. System XYZ shall process classified information.
b. System XYZ shall process unclassified, sensitive information.
c. System XYZ shall process unclassified information.
d. System XYZ shall be accredited in accordance with DoDI 5200.40, DITSCAP

None of the above requirement statements provide enough detail for a bidder to properly assess the system security requirements necessary for certification and accreditation of the automated information system. The bidder normally includes the following type of statements in their response to the RFP and does very little else to assess the impact of IA, in terms of cost and schedule, on their automated information system design.

a. ABC Company will design the XYZ system to process unclassified, sensitive information.
b. ABC Company will design the XYZ system to enable accreditation for processing classified information in accordance with DoDI 5200.40, DITSCAP

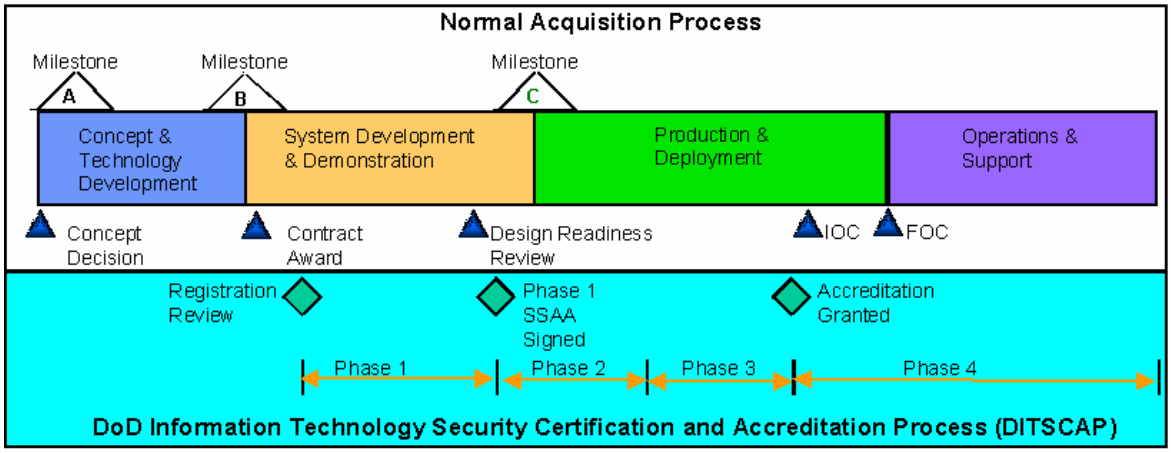

Figure 1 IA as an Afterthought

The government generally accepts these types of responses and the contract is awarded, because the IA staff has not participated in the process.

After Contract Award

Shortly after contract award, either the government, or the contractor begins preparation activities to conduct a Registration Review (RR), which formally begins the DITSCAP. During the preparation activity, information and documentation is collected about the system, which includes capabilities and functions the system will perform, desired interfaces and data flows associated with those interfaces, information to be processed, operational organizations supported, intended operational environment, and operational threat. Typically, this information is contained in the mission needs statement, operational requirements document, system concept of operations document, and system specification. After analysis of this information, the security parameters for the system are determined. Prior to 2003, the security parameters for information systems were the security mode of operation (Dedicated, System High, Multilevel Security, or Compartmented), the sensitivity level of the information to be processed (Unclassified, Sensitive But Unclassified, Confidential, Secret, or Top Secret) and the certification level (Level 1, 2, 3, or 4). Starting in 2003, the security parameters for information systems became the mission assurance category (I, II, or III), the confidentiality level (Classified, Sensitive, or Public), the certification level (Level 1, 2, 3, or 4), and the robustness level (High, Medium, or Basic). The security parameters for the system are presented at the RR.

The Registration Review

The registration review initiates the certification and accreditation process and is a formal meeting between the Designated Approval Authority, Certification Authority, Program Manager, and the User Representative, or their respective representatives, to reach agreement on the following system security parameters:

a. Mission Assurance Category (MAC) – IAW DoDI 8500.2
b. Confidentiality Level - IAW DoDI 8500.2
c. Robustness Levels - IAW DoDI 8500.2
d. Certification Level – IAW DoD 8510.1-M

The RR decisions are documented and this documentation is included in Appendix I of the System Security Authorization Agreement[1] (SSAA). The security parameters agreed to at the RR determine, to a great extent, the security requirements for the system. After completion of the RR, the process of writing the DITSCAP Phase 1 SSAA begins in earnest. Either the government or the contractor may develop the SSAA.

Determination of Security Requirements

One of the tasks during the DITSCAP Phase 1 is the determination of the system's security requirements, which includes the system security requirements that the contractor must meet for a Type accreditation[2] and the system security requirements the fielding site must meet to fully certify and accredit the system for operation at the fielding site, i.e., Site accreditation[3]. National, DoD, and DoD Component level guidance define the security requirements. The regulatory guidance utilized to determine the system's security requirements prior to 2003 has been superseded, as discussed in the IA REGULATORY GUIDANCE EVOLUTION section, and will not be discussed further.

In 2003, DoDI 8500.2 became the main DoD level guidance utilized to determine the system's security requirements. As stated in the Implementation of IA Change within DoD section, DoDI 8500.2 contains a set of IA Controls relevant to each mission assurance category and each confidentiality level. Since the mission assurance category and confidentiality levels were determined and agreed to during the RR, it is a relatively easy task to determine the correct IA Controls for the system. The IA Controls are converted to security requirements ("shall" statements) and are augmented by other DoD guidance and DoD Component level guidance, e.g., AR 25-2, to determine the full set of security requirements necessary to certify and accredit the system. It is at this point that contractual problems which impact cost and schedule arise.

[1] System Security Authorization Agreement is a formal agreement among the DAA, the CA, the IT system User Representative, and the Program Manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

[2] Type accreditation is used when like systems are deployed to multiple locations or there are different DAAs for procurement and the fielding site. The SSAA is prepared for the system software and hardware. Also known as Generic accreditation.

[3] Site accreditation builds on the Type accreditation and provides the necessary assurance that the type accredited software and hardware is correctly installed in an operational environment and meets specified requirements.

Security Requirements Impacts
Since the RR was held after contract award and security was either not considered at all, or not considered in any detail prior to contract award, the security requirements identified during the DITSCAP Phase 1 must be added to the contract.

If the government prepared the SSAA, a contract modification must be executed, between the government and the contractor, to add the security requirements to the contract. Adding the security requirements to the contract after contract award increases the cost and lengthens the schedule for the program.
If the contractor prepared the SSAA, an engineering change proposal (ECP) or baseline change request (BCR) is prepared by the contractor, based upon the identified security requirements, and presented to the government to begin the process to add the security requirements to the contract. The government then prepares and executes a contract modification based upon the ECP or BCR submitted by the contractor. This process also increases the cost and lengthens the schedule for the program.

Additionally, if government funding required to implement the security requirement is not readily available, the program could be canceled, or at a minimum, delayed until funding is identified. These cost and schedule problems can be avoided if IA is accomplished as a forethought, rather than as an afterthought.

Worst Case Scenario
Some programs in the past, and a relatively few programs currently, do not begin implementation of IA until after the design phase or sometimes after the development phase. This compounds the problems described previously. Not only does the program have to accomplish all of the tasks described previously, the implementation of IA at this late date will more than likely impact the system design, which will severely impact the cost and schedule of the program. An even worse case is that the program will attempt to solve the IA problem with bolt-on security. Bolt-on security usually results in a poor security solution for the system, at a very high dollar cost to the program.

IA AS A FORETHOUGHT

IA as a forethought requires involvement of the procurement organization's IA staff in developing the RFP and in determining the system security parameters prior to contract award. When IA is a forethought for an automated information system procurement, the cost and schedule for accomplishing IA is determined prior to contract award, not after. Figure 2 depicts the process discussed in this section with the DITSCAP shown under the normal acquisition cycle process.

Improved Process

The process described in this section is generally applicable to automated information systems that process secret or below information, which do not contain compartmented information. Information systems that process top secret, compartmented, or higher information are not considered because those systems have a different regulatory process.

Prior to Contract Award
After an operational requirements document is approved for an information system, the government procurement team develops a RFP, which may or may not contain a product specification. During RFP development, the IA staff of the procurement organization participates as a member of the RFP development team to provide insight into the IA process and to ensure that IA is given the same level of consideration as the design and development of the system.

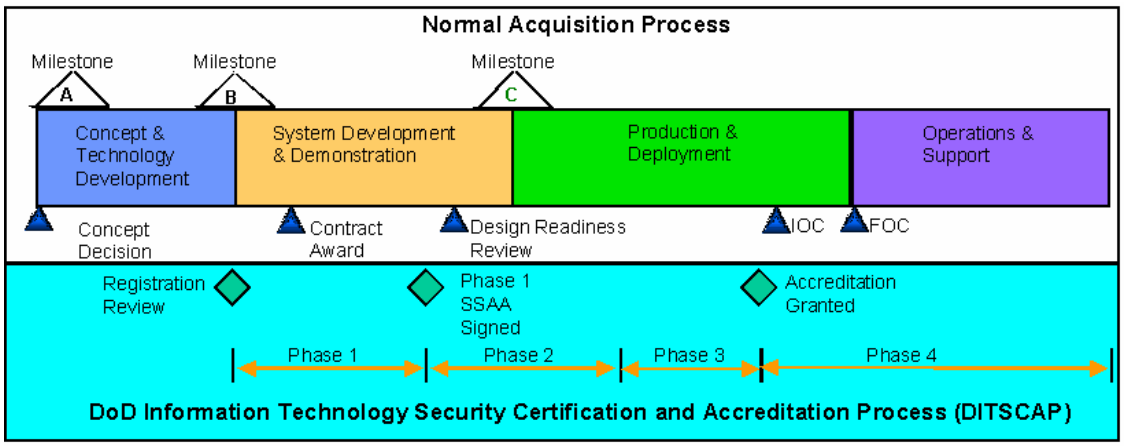

Figure 2 IA as a Forethought

While the RFP is being developed, the IA staff begins preparation activities to conduct a Registration Review (RR) which occurs prior to the release of the RFP. During the RR preparation activity, information and documentation is collected about the system, which includes capabilities and functions the system will perform, desired interfaces and data flows associated with those interfaces, information to be processed, operational organizations supported, intended operational environment, and operational threat. Typically, this information is contained in the mission needs statement, operational requirements document, system concept of operations document, and system specification. After analysis of this information, the security parameters for the system are determined. The security parameters for information systems are the mission assurance category (I, II, or III), the confidentiality level (Classified, Sensitive, or Public), the certification level (Level 1, 2, 3, or 4), and the robustness level (High, Medium, or Basic). Once determined, the security parameters for the system are presented at the RR.

The Registration Review

The registration review initiates the certification and accreditation process and is a formal meeting between the Designated Approval Authority, Certification Authority, Program Manager, and the User Representative, or their respective representatives, to reach agreement on the following system security parameters:

a. Mission Assurance Category (MAC) – IAW DoDI 8500.2
b. Confidentiality Level - IAW DoDI 8500.2
c. Robustness Levels - IAW DoDI 8500.2
d. Certification Level – IAW DoD 8510.1-M

The RR decisions are documented and this documentation is included in Appendix I of the System Security Authorization Agreement (SSAA). The RR decisions are also converted into requirement statements and included in the security section of the RFP or product specification. The security requirement statements should, at a minimum, include the following:

a. System XYZ shall be certified in accordance with the IA Controls for Mission Assurance Category (MAC) __ contained in Attachment __ of Enclosure 4 to DoDI 8500.2
b. System XYZ shall be certified in accordance with the IA Controls for Confidentiality Level __ contained in Attachment __ of Enclosure 4 to DoDI 8500.2
c. System XYZ shall be certified to a Robustness Level of __ in accordance with DoDI 8500.2
d. System XYZ shall be certified in accordance with Certification Level __ in accordance with DoD 8510.1-M
e. System XYZ shall be certified in accordance with the requirements of (Insert the DoD Component level guidance, e.g., AR 25-2).
f. System XYZ shall be accredited in accordance with DoDI 5200.40, DITSCAP and DoD 8510.1-M, DITSCAP Application Manual

In addition to the above security requirement statements, consideration needs to be given to TEMPEST[4], communications security (COMSEC), and Wireless Networks requirements if they are applicable to the system being procured. These security requirement statements provide enough detailed information for the bidders to properly assess the system security requirements necessary for certification and accreditation of the automated information system. The bidders will also be able to determine the cost and schedule to implement the system security requirements and include that information in their proposals.

Alternatively, the government may determine the system security requirements for the Type accreditation of the system based upon the RR selected security parameters and include them in the RFP or product specification. At the same time, the government needs to determine the system security requirements that the fielding site must meet to achieve a Site accreditation. By identifying the system security requirements that the fielding site must meet early in the program, the site is given sufficient time to budget for their accomplishment prior to fielding the system. This method will require more time than generating the security requirement statements; however, it assures that all bidders have a thorough understanding of the security requirements necessary to accomplish a Type certification and accreditation for the system. It also provides the fielding site with adequate time to budget for the accomplishment of the Site accreditation.

Regardless of whether the security requirement statements, or the system security requirements method is used, the IA staff of the procurement organization needs to participate in the evaluation of the submitted proposals to ensure that the proposals adequately address the requirements necessary to achieve a Type

[4] TEMPEST – A short name referring to the evaluation and control of compromising emanations from telecommunications and automated information systems equipment.

certification and accreditation of the system. The IA staff scores the security section of each proposal and provides their findings to the program's selection committee.

After Contract Award

After contract award, either the government or the contractor continues development of the DITSCAP Phase 1 SSAA. Since the RR has already been conducted, the development of the Phase 1 SSAA will require less time than it would have under the processes used in the past. One of the tasks during the DITSCAP Phase 1 is the determination of the system's security requirements for Site accreditation, which includes the system security requirements that the contractor must meet and the system security requirements that the fielding site must meet to fully certify and accredit the system for operation at the fielding site. Since the system security requirements for both the contractor and the fielding site have already been determined prior to contract award, the only task would be to document the total system security requirements in Appendix F of the SSAA.

Security Requirements Impacts

Because the system security requirements for a Type accreditation were identified prior to contract award, the bidders were able to propose the cost and schedule to implement them. In order to award the contract, the government had to identify funds to execute the IA portion of the system. Therefore, there should be no cost or schedule impacts to the program attributable to the system security requirements, under this process.

CONCLUSION

IA regulatory guidance from the DoD and DoD Component levels has changed dramatically over the past two years and is expected to continue to change for the next one or two years. Program Executive Officers, Program Managers, and Product Managers should be familiar with these changes to enable them to understand the impacts of IA on their programs. IA personnel should be thoroughly knowledgeable of the changing regulatory guidance to enable them to properly support their program management.

Executing IA as a forethought rather than as an afterthought will result in savings to the program in terms of cost and schedule. Setting the IA foundation prior to contract award assists both the government and the contractor, and allows the contractor to clearly understand the IA needs of the program for which he is preparing a proposal. After contract award, both the government and the contractor will have a solid IA foundation upon which to build a secure system.

REFERENCES

Department of Defense Directive 8500.1, *Information Assurance (IA)*, October 24, 2002

Department of Defense Instruction 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

Department of Defense Instruction 8510.bb (Draft), *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, March 19, 2004.

Army Regulation 25-2, *Information Assurance*, November 14, 2003

Program Executive Office Simulation, Training, and Instrumentation Basic Accreditation Manual, August 3, 2003