DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

NOV 10 2015

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY FOR ACQUISITION, LOGISTICS AND TECHNOLOGY
ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH, DEVELOPMENT AND ACQUISITION
ASSISTANT SECRETARY OF THE AIR FORCE (ACQUISITION)
DEPARTMENT OF THE ARMY, CHIEF INFORMATION OFFICER
DEPARTMENT OF THE NAVY, CHIEF INFORMATION OFFICER
DEPARTMENT OF THE AIR FORCE, CHIEF INFORMATION OFFICER

SUBJECT: Outline and Guidance for Acquisition Programs' Cybersecurity Strategies

The Clinger-Cohen Act (40 U.S.C. Subtitle III) in the 2001 NDAA §811(P.L. 106-398), DoDI 5000.02, *Operation of the Defense Acquisition System,* and DoDI 8500.01, *Cybersecurity,* set policy to ensure programs have a strategy to implement cybersecurity and manage associated risks. All Acquisition programs acquiring systems containing information technology are required to develop and maintain a Cybersecurity Strategy (formerly the Acquisition Information Assurance Strategy), which is submitted to the cognizant chief information officer for review and approval at milestones and decision points.

The DoD CIO has revised the attached Cybersecurity Strategy Outline and Guidance in order to 1) reflect recent cybersecurity-related policy changes, 2) improve programs' cybersecurity planning, implementation, and communication throughout the lifecycle, and 3) streamline and increase program efficiency by aligning with other Department efforts to better integrate cybersecurity and Acquisition. Programs should use the attached outline and guidance to inform development of their Cybersecurity Strategies, which may be supplemented and tailored to address organizational and individual program needs.

The point of contact for this activity is Mitchell Komaroff, Director of Cybersecurity Implementation and Acquisition Integration, mitchell.komaroff.civ@mail.mil, 703-697-3314.

Richard A. Hale
Deputy Chief Information Officer
for Cybersecurity

Attachment:
As stated

Cc:
OUSD(AT&L)

OUTLINE AND GUIDANCE FOR THE CYBERSECURITY STRATEGY

1. This document provides an outline and high-level guidance on the expectations for the Cybersecurity Strategy as required by the Clinger-Cohen Act (40 U.S.C. Subtitle III) in the 2001 NDAA §811(P.L. 106-398), DoDI 5000.02 – *Operation of the Defense Acquisition System*, and DoDI 8500.01 – *Cybersecurity*. This document replaces the Acquisition Information Assurance (IA) Strategy outlined in DoDI 8580.1 - *Information Assurance (IA) in the Defense Acquisition System*. This revision reflects the thrust of integrating cybersecurity and acquisition in these new policies, as well as DoDI 8510.01 - *Risk Management Framework (RMF) for DoD Information Technology (IT)* and the DoD *Program Manager's (PM) Guidebook for Integrating the Cybersecurity RMF into the System Acquisition Lifecycle*.

2. The Cybersecurity Strategy is a required acquisition program document created and maintained by the Program Office and appended to the Program Protection Plan (PPP). The PM and team develops the Cybersecurity Strategy as early as possible, and continually updates and maintains it to mature at a rate commensurate with that of the program. The Cybersecurity Strategy reflects both the program's long-term approach for, and implementation of cybersecurity throughout the program lifecycle. The Cybersecurity Strategy is a tool for PMs, Authorizing Officials (AO) or Authorizing Official Designated Representatives (AODR), and relevant review and approval authorities to plan for, identify, assess, mitigate, and manage risks as systems mature.

3. The PM submits the Cybersecurity Strategy for review by the AO/AODR, and review and approval by the cognizant CIO at MS A; and updates and re-submits for review and approval at development RFP release decision, MS B, MS C, and FRP/FDD. For ACAT ID and IAM programs, DoD CIO is the approval authority. Approval of the Cybersecurity Strategy does not override complementary required policy processes.

4. The Cybersecurity Strategy consolidates elements of various program initiatives and activities relating to cybersecurity planning, implementation, and risk management. The reuse of existing analysis and documentation is strongly encouraged where practical for the development of the Cybersecurity Strategy. It is incumbent on the submitting Program Office to ensure any referenced information is readily available to the document review/approval chain by providing copies of any supporting documents upon request, including requirements baselines, systems engineering, test, and RMF documentation. Classified annexes may be appended as needed.

5. Program Offices should use the following principles to ensure the document is useful as a plan and working document for the program, and to support cybersecurity and acquisition review and approval functions. These principles form the basis of CIO evaluation criteria in review of Cybersecurity Strategies:

    a. Evidence of comprehensive analysis, including System Security Engineering (SSE), Trusted Systems and Networks (TSN) Analysis, and system survivability, supporting the planning and implementation of cybersecurity on the system, including the intended CONOPS, operating environment and tempo, understanding of expected level of threat leading to the determination of adequate system cybersecurity implementation and achievement of desired operational outcomes.
    b. Evidence of traceability between security controls and the baselines (functional, allocated, and product), and understanding of the balance between risks and requirements trades.

c. Consideration of cybersecurity in relation to the interdependency of this system with the system of systems in which it is intended to operate; the degree to which the capability depends on cybersecurity to perform its key functions and missions.
d. Planning for cybersecurity testing and evaluation throughout the acquisition lifecycle, including testing of security controls in accordance with the RMF; ensuring cybersecurity requirements are testable and measurable.
e. Evidence and understanding of ongoing risk management, including residual risks stemming from the failure to mitigate identified cybersecurity risks and vulnerabilities.

6. Program Offices should utilize the following outline and the above principles in the preparation of their Cybersecurity Strategy documentation. As the document is updated throughout the lifecycle, sections should emphasize changes from previous Strategy submittal. The outline section sub-headings on the next pages contain short descriptions to guide strategy development and recommend the level of detail for the documentation, including suggested approximate page count. Specifically, where sections ask for documentation to "list", "describe", or "discuss" requested information:
    - "List" requires straightforward identification of information;
    - "Describe" requires a brief description, often focused on the process;
    - "Discuss" should contain a more detailed narrative.

    In addition to the outline, the attached Progress Summary referenced in section IV (A) should be used to convey completion of RMF and acquisition cybersecurity activities and will be submitted with each Cybersecurity Strategy to inform CIO review and approval. For additional guidance on content, resources, and references for the Cybersecurity Strategy, refer to the RMF Knowledge Service (https://rmfks.osd.mil).

Outline
(PROGRAM NAME) Cybersecurity Strategy (Expectation: 20-30 pages)
Date of last update:
Classification level:

I. Introduction: *(3 pages)*
   A. Executive Summary – *Describe the program's Cybersecurity Strategy in summary, including authors and contributors, and the status of its implementation.*
   B. Program Information – *List the Acquisition Category (ACAT) level of the program, current phase within the Acquisition lifecycle, next major milestone decision and date, and any other relevant cybersecurity program information, including system type determination (e.g. Information System, Platform IT (PIT) System).*
   C. System Description – *Describe the system being acquired and its intended operational environment, major system functions, subsystems, etc.*

II. Sources of Cybersecurity Requirements: *(2 pages)*
   A. System Categorization – *Describe approach for completing system categorization, including who is involved and responsible, rationale, and results of system categorization, completed IAW DoDI 8510.01 and CNSSI No. 1253. Include expected list of information types and any planned or applicable overlays.*
   B. Initial Control Selection – *Describe major system performance constraints that result in substantial deviations from the baseline control set or applicable overlays. Describe process for identifying security controls deemed "Not Applicable".*
   C. JCIDS specified requirements – *Describe cyber survivability and cybersecurity requirements as defined in the Initial Capability Document (ICD), Capability Development Document (CDD), and Capability Production Document (CPD) as part of the System Survivability Key Performance Parameter (KPP) and any other cybersecurity capability requirements defined by any other KPPs, key system attributes, or additional performance attributes. Include the applicability or non-applicability of the System Survivability KPP as it applies to cybersecurity or survivability in a cyber-contested environment.*
   D. Other requirements – *Describe any additional cybersecurity requirements from other sources, including organization or Service-level requirements, and technical requirements (e.g. COMSEC, Cross-Domain).*

III. Cybersecurity Approach:
   A. Management Approach (2 pages)
      1. Stakeholder Communication and Documentation – *Describe methods and periodicity of communication between program and AO/AODR, including the communication of risks and changes affecting risk posture. Describe how the program will plan for stakeholder input (e.g. Integrated Product Teams (IPT), working groups) and plan for assembly, dissemination, and coordination of required documentation including documentation of cybersecurity risks. Describe the process for AO (or designee) review of the Cybersecurity Strategy.*
      2. Acquisition of Cybersecurity Capabilities and Support - *Describe the methods to incorporate cybersecurity requirements in contracting, specifically regarding contractor functions. Include contractor responsibilities, if any.*

      3. System Assessment and Authorization

a. Current approach

Describe your current approach to attaining authorization for your system. List whether an automated tool (e.g. eMASS) is being used. List key role assignments. Describe authorization boundary. Include milestones and schedule information with expected outcomes.

b. Transition to Risk Management Framework (RMF)

Describe your intent to transition to the RMF to comply with the DoD scheduled transition. Include milestones and schedule information with expected outcomes. If your current approach (above) is the RMF for DoD IT, please list, "Transition In progress" or "Transition Complete."

B. Technical Approach (5 pages)

1. System Design and Architecture - *Describe the high-level plan to integrate cybersecurity into system architecture and design; discuss the processes for identifying and applying overlays, for identifying which controls will be inherited, and for any other initial tailoring activities, including stakeholder involvement and any supporting analysis.*
2. Requirements Traceability - *Describe process and mechanism that will be used to ensure requirements will trace to controls throughout the system lifecycle. Describe how baselines (functional, allocated, and product) will be traced to security controls throughout the lifecycle. Describe how cybersecurity developmental T&E and operational T&E requirements trace to test plans (e.g. Test and Evaluation Master Plan, Security Assessment Plan).*
3. Risk Assessments – *Describe plan for periodic RMF risk assessments (including periodicity, stakeholders, and methodology); Describe how they will be integrated with other risk assessment activities, including TSN Analysis (including criticality analysis), programmatic risk assessments, and operational testing.*
4. External Connections – *Discuss the external connections of the system and the approach for protection provided. Include discussion of vulnerabilities introduced by external systems or infrastructure and their interfaces. Include dependencies on other external systems and interfaces to/with those systems, and their authorization status.*
5. Inherited Protection - *List functions that will be inherited from other sources.*

IV. Cybersecurity Implementation: (5 pages)

A. Progress Summary – *Use attached progress summary to check-off completed activities.*

B. Technical Implementation

1. System Design and Architecture - *Discuss system security architecture using a technical narrative; or in lieu of a description, provide an illustrative system view of the security architecture. Describe high-level deviations from security controls and baselines. Describe the impact of those deviations and corresponding mitigations. List status of completion of testing activities and reference testing documentation.*
2. Requirements Traceability - *Describe the status of allocation of security functions and their traceability to security controls. Include summary of requirements traceability from the detailed performance requirements to engineering approach.*
3. TSN Analysis – *Describe how results of TSN Analysis have informed the implementation of cybersecurity, including design, architecture, engineering changes and other mitigations for the protection of critical functions.*

4. RMF Artifacts - *List status of RMF artifact implementation. (e.g., Security Plan, Security Assessment Plan, Security Assessment Report, Plan of Action and Milestones, Authorization Decision (Security Authorization Package))*
5. Risk Assessments – *Describe key risk decisions and trades that have been made as a result of the risk assessments.*
6. Other – *Describe any other technical considerations.*
7. Cybersecurity entry and exit criteria – *Describe method to develop entry/exit criteria for Systems Engineering Technical Review (SETR) events and status of development and approval since last milestone. List any criteria that were not met and describe plan to address unmet criteria.*

V. Risk Management: (5 pages)

A. Cybersecurity risks
   1. *System performance risks - List and describe any significant outstanding technical cybersecurity risks, and proposed solutions and/or mitigation strategies including technical solutions and/or tactics, techniques, and procedures. Discuss the impact of failure to resolve any residual risk in terms of system performance consequences of cybersecurity risk, and mission impact. Discuss communication of risks and impacts to key risk stakeholders.*
   2. *Risks to program cost and schedule - List and describe significant risks to cost and schedule of program related to failure to meet cybersecurity requirements. List risks in the program risk register. Include failure to achieve thresholds and objectives in governing documents.*

B. Proposed Solutions and Mitigations - *List actions from previous Cybersecurity Strategy reviews, and timeline to complete. Discuss any issues and risks associated with failure to resolve them.*

C. AO/AODR Comments – *AO/AODR provides comments on cybersecurity risk posture. Include date and approval status of RMF Security Plan and RMF authorization decision (if applicable).*

VI. Policy and Guidance: (Less than a page) *List the primary policies and guidance employed by the program for preparing and executing the Cybersecurity Strategy, and supporting activities; including both OSD and Component-level policies and guidance.*

VII. Point of Contact(s): (Less than a page) *List responsible POC and other stakeholders including name and contact information for the Program Office individuals responsible for the Cybersecurity Strategy document, PM, AO, and other relevant Cybersecurity Strategy stakeholders (e.g. AODR, Security Control Assessor, Information System Security Manager, Chief Engineer, System Security Engineer).*

VIII. Other considerations: (Less than a page) *Area for additional consideration as appropriate, including special considerations, or alternate process agreements (with stakeholders and any special arrangements). Document any agreements with DoD CIO or at the Service-level related to the Cybersecurity Strategy.*

IX. Signature Page: (Less than a page) *Include a signature page containing all individuals who have reviewed and approved the Cybersecurity Strategy, including the PM, AO, and cognizant CIO.*

CYBERSECURITY STRATEGY PROGRESS SUMMARY

Activities listed in the progress summary below are not intended to be a comprehensive checklist for all required cybersecurity activities to be performed within a program. How and when cybersecurity activities are implemented should be tailored to meet the requirements and needs of each program. The Cybersecurity Strategy Outline and Progress Summary will be used together as a basis for cognizant CIO review and assessment.

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
Materiel Development Decision (MDD)			**DoDI 5000.02**	
Information Systems Security Manager (ISSM) appointed and qualifications of system security engineer(s) ensured			DoDI 8510.01	
Security Plan initiated			DoDI 8510.01; *See RMF Knowledge Service for template*	
System categorized (identify potential impact levels due to the loss of confidentiality, integrity, and availability) to support Initial Capabilities Document (ICD) development			DoDI 8510.01; *CNSSI 1253*	
ISSM and System Security Engineer (SSE) assessed cybersecurity risk per criteria in Analysis of Alternatives (AoA) study plan and cybersecurity capability requirements from the ICD			DoDI 5000.02	
Sponsor and Joint Staff developed preferred cybersecurity risk solutions			DoDI 5000.02	
Chief Engineer (CE), ISSM, User Representative (UR), Sponsor, CIO and SSE identified applicable cybersecurity enterprise architectures in the system conceptual design			DoDI 8510.01; DoDI 5000.02	
Security control baseline and overlays selected and tailoring begun			DoDI 8510.01; *CNSSI 1253*	
CE and SSE ensured that the initial security controls baseline traces to the preliminary system performance specifications that comprise the preliminary functional baseline			DoDI 8510.01	
Initial Trusted Systems and Networks (TSN) Analysis conducted: CE and SSE conducted TSN Analysis focused at mission level, including Criticality Analysis (CA) to identify critical functions, Threat Assessment (TA), Vulnerability Assessment (VA), TSN Risk Assessment, and countermeasure selection			DoDI 5200.44; DoDI 5000.02	
Initial Cybersecurity Risk Assessment completed: CE and ISSM conducted cybersecurity risk assessment using the mission context as described in the ICD with consideration of likelihood of attack, as well as results from the TSN Risk Assessment			DoDI 8510.01	
Alternative Systems Review (ASR); best practice but not required			DoDI 5000.2 (DAG Chapter 4)	
Sponsor briefed Joint Staff (JS) Functional Capabilities Board (FCB); AO/AODR informed; JROC provided informed advice to the MDA			CJCSI 3170.01H, JCIDS, and JCIDS Manual	
Cybersecurity capability requirements documented and security controls planned to meet those requirements			DoDI 8510.01	
System-level continuous monitoring strategy developed			DoDI 8510.01	

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
System registered			DoDI 8510.01	
Security Plan approved by AO/AODR			DoDI 8510.01	
Continuous Monitoring Strategy approved by AO/AODR			DoDI 8510.01	
Cybersecurity Strategy submitted to AO			DoDI 5000.02	
Milestone A			**Reference: DoDI 5000.02**	
Milestone A Exit Criteria Approved			DoDI 5000.02	
Derived cybersecurity system-level requirements refined			CJCSI 3170.01H; DoDI 5000.02 (DAG Chapter 4)	
Derived cybersecurity requirements refined and coordinated among the system's Program Protection Plan (PPP), Cybersecurity Strategy, Security Plan, and specifications for the technical solution in preparation for the SRR			DoDI 8510.01 DoDI 5000.02	
TSN analysis updated and focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection (in coordination with SCA and AO/AODR)			DoDI 5200.44 DoDI 5000.02	
Cybersecurity risk assessment updated (Threat, Vulnerability, Likelihood, and Impact), including results from the TSN analysis			DoDI 8510.01	
System Requirements Review (SRR)			DoDI 5000.2 (DAG Chapter 4)	
System specifications refined by translating and deriving cybersecurity specifications from the system's cybersecurity capability requirements (both explicitly specified and implicitly derived)			CJCSI 3170.01H; DoDI 5000.02 (DAG Chapter 4)	
System Functional Review (SFR)			DoDI 5000.2 (DAG Chapter 4)	
System functional baseline evaluated to satisfy the draft CDD's cybersecurity requirements; functional requirements and verification methods support achievement of performance requirements in the SFR; and that functional requirements and verification methods support the initial EMD RFP development			CJCSI 3170.01H	
Test and Evaluation Master Plan (TEMP) aligned with the Security Assessment Plan, Systems Engineering Plan (SEP), PPP, Cybersecurity Strategy, System Threat Assessment Report (STAR), and Acquisition Strategy			DoDI 5000.02	
SCA developed the Security Assessment Plan. Security Assessment Plan aligned with the TEMP, SEP, PPP, Cybersecurity Strategy, and acquisition strategy			DoDI 8510.01	
SEP and PPP updated and aligned with the TEMP, Security Assessment Plan, and acquisition strategy			DoDI 5000.02	
EMD RFP developed including cybersecurity language, and acquisition strategy updated and aligned with the TEMP, Security Assessment Plan, and SEP			DoDI 5000.02	
Developmental RFP Release			**Reference: DoDI 5000.02**	
Allocated baseline defined (including cybersecurity considerations)			DoDI 5000.02	

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
Preliminary Design Review (PDR)			DoDI 5000.02	
Cybersecurity Strategy submitted to AO			DoDI 5000.02	
Milestone B – Security Plan and Cybersecurity Strategy submitted to CIO			**Reference: DoDI 5000.02**	
Milestone B Exit Criteria Approved			DoDI 5000.02	
Cybersecurity requirements mapped and allocated to the hardware and software design for the system as part of the overall system development process to support test and evaluation planning			DoDI 5000.02	
Attack surface characterized and assessment begun for cybersecurity planning and performing component and system integration testing			DoDI 5000.2 (DAG Chapter 9)	
Critical Design Review (CDR) entrance criteria met for cybersecurity baseline design and all cybersecurity requirements reflected in the product baseline including the design			DoDI 5000.02 (DAG Chapter 4)	
CDR			DoDI 5000.02	
TSN analysis updated and focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection (in coordination with SCA and AO/AODR)			DoDI 5200.44 DoDI 5000.02	
Cybersecurity risk assessment updated (Threat, Vulnerability, Likelihood, and Impact), including results from the TSN analysis			DoDI 8510.01	
Vulnerability analysis conducted and testing performed to evaluate the system's cybersecurity in a mission context using realistic threat exploitation techniques			DoDI 5000.02	
Developmental test and evaluation (DT&E) events conducted to demonstrate system maturity and readiness to begin production and preparedness for operational test and evaluation and/or deployment and sustainment activities; coordinated with SCA; AO/AODR, DT&E, and OT&E staff.			DoDI 8510.01	
Interim Authorization to Test (IATT) issued (If necessary)			DoDI 5000.2 (DAG Chapter 9)	
DT&E assessment prepared as input to Milestone C Decision			DoDI 5000.02	
Cybersecurity-derived requirements implemented and verified in the hardware and software design for transition to the development and manufacturing environment			DoDI 5000.02(DAG Chapter 4)	
Functional Configuration Audit (FCA)			DoDI 5000.2 (DAG Chapter 4)	
System Verification Review (SVR)			DoDI 5000.2 (DAG Chapter 4)	
Production Readiness Review (PRR)			DoDI 5000.2 (DAG Chapter 4)	
Security controls assessed			DoDI 8510.01	
SCA prepared the Security Assessment Report (SAR)			DoDI 8510.01	
Initial remediation actions conducted			DoDI 8510.01	
RMF Plan of Action and Milestones (POA&M) prepared			DoDI 8510.01	
Security Authorization Package assembled (Security Plan, SAR, & POA&M)			DoDI 8510.01	
Cybersecurity Strategy submitted to AO			DoDI 5000.02	

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
Milestone C			**Reference: DoDI 5000.02**	
Milestone C Exit Criteria Approved			DoDI 5000.02	
Network connection approval package submitted			DoDI 8510.01	
Cybersecurity risk assessment updated for deficiencies/weaknesses			DoDI 8510.01	
Cybersecurity risk assessment results documented with corrective actions in the RMF POA&M			DoDI 8510.01	
AO/AODR provided with an updated risk assessment, if cybersecurity risk increases after IOT&E, to determine if reauthorization is necessary			DoDI 8510.01	
TSN analysis updated and focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection (in coordination with SCA and AO/AODR)			DoDI 5200.44 DoDI 5000.02	
Any deficiencies addressed prior to the Full-Rate Production (FRP) or Full Deployment Decision (FDD)			DoDI 5000.02	
CS activities included in Lifecycle Sustainment Plan (LCSP)			DoDI 5000.02	
Physical Configuration Audit (PCA)			DoDI 5000.02 (DAG Chapter 4)	
FRP or FDD – Security Plan and Cybersecurity Strategy submitted to CIO			**Reference: DoDI 5000.02**	
FRP/FDD Exit Criteria Approved			DoDI 5000.02	
System-level Continuous Monitoring Plan (developed in MS A) and annual review cycle implemented			DoDI 8510.01	
LCSP, Security Plan, POA&M, PPP, and Cybersecurity Strategy updated based on evolving cybersecurity threats and required corrective actions, while the program is in sustainment			DoDI 5000.02	
Maintain all cybersecurity requirements included in the Security Plan. Supporting activities may include: ▪ Implement Information Assurance Vulnerability Alerts (IAVAs) ▪ Apply software patches and updates ▪ Update and maintain anti-virus/HIDS signatures ▪ Apply Warning Orders and Operation Orders ▪ Update or replace hardware ▪ Apply firmware updates ▪ Reauthorization as needed per the DoD RMF for IT requirements ▪ Maintain local site infrastructure, facility, physical, and procedural security requirements			DoDI 8510.01; *See RMF KS for template*	
TSN analysis updated and focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection (in coordination with SCA and AO/AODR)			DoDI 5200.44 DoDI 5000.02	
Cybersecurity risk assessment updated (Threat, Vulnerability, Likelihood, and Impact), including results from the TSN analysis;			DoDI 8510.01	

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
In-Service Review (ISR) *Additional ISRs during O&S until decommissioning are typically critical for systems that change frequently, such as commercial-off-the-shelf and software-intensive systems*			DoDI 5000.02 (DAG Chapter 4)	
After sustainment, disposal phase implemented. *A risk assessment for decommissioned systems should be conducted and the appropriate steps taken to ensure that residual classified, sensitive or privacy information is not exposed.*			DoDI 5000.02	
For systems inheriting controls from a decommissioned system, ensured "disinherited" controls are implemented elsewhere			DoDI 8510.01	

Legend:

AO	Authorizing Official
AOA	Analysis of Alternatives
AODR	Authorizing Official Designated Representative
CDT	Chief Developmental Tester
CE	Chief Engineer/Lead Systems Engineer
CIO	DoD CIO or Component CIO
DIA	Defense Intelligence Agency
D/SI	Developer or System Integrator
IO	Information Owner
ISSM	Information System Security Manager
JROC	Joint Requirements Oversight Council
MDA	Milestone Decision Authority
OTA	Operational Test Agency
POA&M	Plan of Actions and Milestones
PM	Program Manager
SCA	Security Control Assessor
SOW	Statement of Work
Sponsor	Requirements Sponsor, Functional Sponsor or Mission Owner
SSE	Security System Engineer
UR	User Representative