Department of the Army
Pamphlet 25–2–11

Information Management: Army Cybersecurity

Cybersecurity Strategy for Programs of Record

Headquarters
Department of the Army
Washington, DC
15 April 2019

UNCLASSIFIED

SUMMARY

DA PAM 25–2–11
Cybersecurity Strategy for Programs of Record

This new Department of the Army Pamphlet, dated 15 April 2019--

o Provides guidance on the Cybersecurity Strategy for Programs of Record review and approval processes and procedures within the Department of the Army (throughout).

o Issues instructions for Army organizations to implement cybersecurity strategy effectively (throughout).

Headquarters
Department of the Army
Washington, DC
15 April 2019

Department of the Army Pamphlet 25–2–11

Information Management : Army Cybersecurity

Cybersecurity Strategy for Programs of Record

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

Kathleen S. Miller

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a new Department of the Army Pamphlet.

Summary. This pamphlet provides guidance for the vetting and approval of the Cybersecurity Strategy for Programs of Record within the Department of the Army. This pamphlet provides directive procedures and guidance to implement DODI 8510.01, DODI 8500.01, AR 25–2, and the DOD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework into the System Acquisition Lifecycle.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this pamphlet is the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the respective policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Office of the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107.

Distribution. This publication is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Contents—Continued

Chapter 1
Introduction

1–1. Purpose

The purpose of the Cybersecurity Strategy (CSS) for Programs of Record (POR) is to ensure compliance with the statutory requirements of the Title 40, United States Code (USC), Subtitle III (Clinger-Cohen Act) and related legislation, as implemented by DODI 5000.02. The CSS is an appendix to the program protection plan (PPP) that satisfies the statutory requirement in Section 811 of Public Law 106–398 for mission-essential and mission-critical information technology (IT) systems. The program manager (PM) develops the acquisition CSS to help the program office (PO), organize and coordinate its overall cybersecurity approach to identifying and satisfying cybersecurity requirements consistent with Department of Defense (DOD) and Army policies, standards, and architectures for all new systems or networks. This document replaces the acquisition information assurance (IA) strategy originally required by DODI 8580.1 to reflect guidance in DODI 5000.02, DODI 8500.01, and DODI 8510.01.

1–2. References and forms

See appendix A.

1–3. Explanation of abbreviations and terms

See the glossary.

1–4. Applicability

This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Chapter 2
Cybersecurity Strategy for Programs of Record Management and Approval Processes

2–1. Cybersecurity strategy for programs of record management process

a. The CSS for POR is a required acquisition program as documented by DODI 5000.02, DODI 5000.75, and DODI 5200.39. All acquisitions of systems utilizing IT, including National Security Systems and legacy systems, must have a CSS. The CSS originates from the PM and is maintained by the PO. Beginning at Milestone A, the PM will submit the CSS to the Army Chief Information Officer/G6 (CIO/G–6) for review and approval prior to milestone decisions or contract awards. The PM will submit the program's CSS as part of every PPP. The CSS will be updated, as necessary, at each program milestone, full-rate production (FRP) decision, or full deployment decision (FDD) with major changes to the system. The CSS will be an annex to the PPP. The PM will develop the CSS as early as possible in the acquisition process, submit for approval prior to Milestone A, and update and re-submit for approval at Request for Proposal (RFP) release, Milestone B, Milestone C, and FRP/FDD. The CSS is an iterative document that reflects the program's long-term approach to, and its implementation of, cybersecurity throughout the program life cycle. The CSS should be used as a tool for the PM, authorizing officials (AOs), and cybersecurity and acquisition oversight authorities to plan for, document, assess, mitigate, and manage risks as the program matures. The PM will update and maintain the CSS and ensure it matures at a rate commensurate with that of the program life cycle.

b. The CSS requires the Program Information System Security Manager (ISSM–P) (formerly Information Assurance Program Manager) supporting the AO, to be involved early in the Acquisition Life Cycle Process. The ISSM–P must be engaged in initial program planning meetings to support—

(1) Defining the system.

(2) Assigning responsibilities.

(3) Determining life cycle costs.

(4) Incorporating system security engineering into the system design.

c. The CSS consolidates elements of various program initiatives and activities related to cybersecurity planning, implementation, and risk management. The reuse of existing analysis and documentation is strongly encouraged where practical for the development of the CSS, to reduce redundancy. The submitting PO must ensure any referenced information is readily available to the document review/approval chain, to include—

(1) Acquisition baselines.

(2) Systems engineering.

(3) Cybersecurity testing.

(4) Risk management framework (RMF) documentation (for example, System Categorization, Security Plan, Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), Test and Evaluation Master Plan (TEMP), PPP, and so on). Classified annexes may be appended as needed.

d. Although other key documents can be referenced within the CSS to identify supplemental or supporting information, the CSS will contain sufficient internal content to communicate clearly the strategy to the reader. The CSS should be as clear and concise as possible while providing enough information to detail the program's strategy to implement cybersecurity throughout the program's life cycle. The objective is to create a document that clearly conveys the intent of the program to comply with DOD and Army policy, standards, and architecture.

e. POs will adhere to 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/G–6 evaluation criteria in review of CSSs—

(1) Evidence of comprehensive analysis, to include—

(a) System Security Engineering.

(b) Trusted Systems and Networks (TSN) analysis.

(c) System survivability, supporting the planning and implementation of cybersecurity on the system, to include the intended concept of operations, operating environment, and tempo.

(d) Understanding of the expected level of threat, leading to the determination of adequate system cybersecurity implementation and achievement of desired operational outcomes.

(2) Evidence of traceability between security controls and the baselines (functional, allocated, and product), and understanding of the balance between risks and requirements.

(3) 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.

(4) Planning for cybersecurity testing and evaluation throughout the acquisition lifecycle, to include testing of security controls in accordance with the RMF, and ensuring cybersecurity requirements are testable and measurable.

(5) Evidence and understanding of ongoing risk management, to include residual risks stemming from the failure to mitigate identified cybersecurity risks and vulnerabilities.

(6) The CSS applies to all Acquisition Categories (ACATs) and will be included as an annex to the PPP. The lack of an Army approved CSS will adversely affect the approval of the PPP.

2–2. Cybersecurity strategy for programs of record review and approval process

a. Submit the CSS for review and approval to the Army CIO/G–6 Cybersecurity Directorate's CSS team mailbox at usarmy.pentagon.hqda-cio-g-6.mbx.cybersecurity-strategy-team@mail.mil, prior to milestone decisions and contract awards, in accordance with the requirements detailed in DODI 5000.02. Cybersecurity strategies for Defense Business Systems are mandated under DODI 5000.75. Submissions require a minimum of 120 days prior to the milestone decision date in order to allow sufficient time for Army CIO/G–6 and DOD CIO review.

b. The Army CIO/G–6 Cybersecurity Directorate review panel, comprised of members from the Cybersecurity Directorate, DOD CIO, U.S. Army Cyber Command, will conduct an initial review of the strategy and provide comments back to the PM within 30 working days after submission.

c. The cybersecurity strategy must be available for review and approval at all acquisition milestone decisions. PMs must have an updated and approved CSS prior to Milestones A, B, and C, to include FRP and FDD.

d. In acquisition categories ID, IC, IA, IAM, and IAC programs, the DOD CIO will review and approve the CSS prior to milestone decisions or contract awards.

e. In ACAT II programs, the Army CIO/G–6 will review and approve the CSS prior to milestone decisions or contract awards.

f. In ACAT III-level programs, the Army CIO/G–6 delegates the approval authority to the responsible program executive officers (PEOs) and Army commands for all mission support and customer programs where the PEO has been designated as the milestone decision authority (MDA). As an annex to the PPP, the CSS elaborates on the approach, and cybersecurity risks and countermeasures employed on the system. Approval of the CSS does not override supplemental, required policy processes.

g. In ACAT III, CSSs approved under this delegation will be verified for statutory and regulatory compliance by the MDA and a copy of the review and approval documentation will be provided to the Army CIO/G–6 Cybersecurity Directorate, SAIS–CBA.

h. The PM submits the CSS for review to the AO or authorizing official designated representative (AODR), in coordination with the AO—and review and approval by the Army CIO/G–6 at Milestone A; and updates and re-submits for review and approval at development RFP release decision, Milestone B, Milestone C, and FRP/FDD. Approval of the CSS does not override supplemental required policy processes.

(1) The PM will resubmit the CSS and signature page to the Army CIO/G–6 Cybersecurity Directorate for final staffing and approval within 30 working days of the review and after all comments have been adjudicated.

(2) The final staffing and approval of the CSS will be completed by the Army CIO/G–6 within 30 working days after final submission (applies to ACAT I and ACAT II programs only).

i. Below are the minimum requirements the CSS must contain at each milestone and throughout its life cycle:

(1) CSS for POR template (see appendix B) to assist in the development of the CSS document for satisfying statutory review requirements.

(2) Address all sections of the template. If a section does not apply, it must be justified in writing.

(3) If the program is in the early stages of development and the section is not applicable, or required information is not known at the time, indicate at what stage the information will be applicable or known.

(4) If a program cannot maintain functionality, or cannot support one of the cybersecurity requirements, then this failure becomes a cybersecurity shortfall and must be documented in the CSS.

(5) If there are no significant changes in the CSS between subsequent program reviews beyond Milestone C, coordinate with Army CIO/G–6 Cybersecurity Directorate to obtain a memorandum for record that the CSS is still valid.

(6) The CSS will undergo periodic revisions and, as such, will change over time as the program evolves or until the system is retired or phased out.

2–3. Milestone requirements

a. Guidelines. The following are reasonable, suggested guidelines for CSS for POR development:

(1) Milestone A (7 pages).

(2) Milestone B or C (15 pages).

(3) Full-rate production or full deployment decision (15 pages).

Note. The tables of content, acronym lists, signature sheets, and executive summaries do not count against the page limitations.

b. Milestone A.

(1) At Milestone A, prior to the technology development phase of the DOD acquisition process, the CSS will mainly focus on the cybersecurity requirements set forth in the requirements document(s) and the methodology being employed.

(2) Complete all Milestone A sections of the CSS for POR template (7 pages).

(3) The table of contents, acronym lists, signature sheets, and executive summaries do not count against the page limitations.

(4) Identify the ACAT level of the program. Identify current acquisition life cycle phase and milestone decision dates. Identify whether the system has been designated mission-critical, mission-essential, or mission-support, in accordance with AR 25–2 and DODI 5000.02 (section 1 of the template).

(5) Provide the name and contact information for the ISSM–P supporting the AO. This person will interface with the Army CIO/G–6 Cybersecurity Directorate for any questions about the CSS document.

(6) Plan for the integrated use of modeling and simulation (M&S) throughout the life cycle of the CSS. Such planning should encompass development of digital product descriptions; verification, validation, and accreditation; and collaboration with the test and evaluation (T&E), experimentation, requirements, logistics, M&S, systems engineering, and training communities so that information developed via M&S efforts will lead to more informed decision making.

c. Milestone B.

(1) At Milestone B, prior to the engineering and manufacturing development phase of the acquisition process, the CSS will address the cybersecurity requirements set forth in the requirements document, focusing on how those cybersecurity requirements are being satisfied.

(2) Complete all Milestone A and B sections of the template (15 pages).

(3) The table of contents, acronym lists, signature sheets, and executive summaries do not count against the page limitations.

(4) Continue to identify current acquisition life cycle phase and milestone decision dates. Identify whether the system has been designated mission-critical, mission-essential, or mission-support, in accordance with AR 25–2 and DODI 5000.02 (section 1 of the template).

(5) Identify cybersecurity requirements for developmental test, and evaluation (DT&E). These should include mitigation of applicable common vulnerabilities.

(a) Integrate cybersecurity into DT&E events and/or plan for dedicated cybersecurity test events as appropriate.

(b) Identify cyber threats to be emulated in test events.

(c) Identify potential impact categorization (low, moderate, or high) resulting from a loss of confidentiality, integrity, and availability.

(d) Identify cybersecurity DT&E resources.

1. Cyber range resources (for example, National Cyber Range, DOD IA Range, or the Joint Information Operations Range).

2. Modeling and simulation or tools for cybersecurity.

d. Milestone C.

(1) At Milestone C, and prior to the production and deployment phase of the acquisition process, the CSS will address the cybersecurity requirements set forth in the requirements documents focusing on how cybersecurity requirements have been implemented.

(2) Complete all Milestone A, B, and C sections of the template (15 pages).

(3) The table of contents, acronym lists, signature sheets and executive summaries do not count against the page limitations.

(4) Maintain the system's security posture throughout its life cycle.

(5) Update the strategy, as required.

e. Full-rate production or full-deployment decision.

(1) At FRP/FDD, the CSS requires demonstrated control of the manufacturing process, acceptable performance and reliability, and the establishment of adequate sustainment and support.

(2) Complete all Milestone A, B, and C sections of the template (15 pages).

(3) The table of contents, acronym lists, signature sheets, and executive summaries do not count against the page limitations.

(4) Maintain the system's security posture throughout its life cycle.

(5) Update the strategy, as required.

f. Guidance. Additional guidance on content, resources, and references for the CSS, refer to the risk management framework Knowledge Service Reference Library (https://rmfks.osd.mil).

Appendix A

References

Section I

Required Publications

The following publications are available on the APD website (https://armypubs.army.mil) unless otherwise stated. DOD publications are available at http://dtic.mil/whs/directives.

AR 25–2
Army Cybersecurity (Cited in title page.)

DODI 5000.02
Operation of the Defense Acquisition System (Cited in para 1–1.)

DODI 5000.75
Business Systems Requirements and Acquisition (Cited in para 2–1*a*.)

DODI 5200.39
Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E) (Cited in para 2–1*a.)*

DODI 8500.01
Cybersecurity (Cited in title page.)

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT) (Cited in title page.)

DODI 8580.1
Information Assurance (IA) in the Defense Acquisition System (Cited in para 1–1.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 25–1
Army Information Technology
AR 25–30
Army Publishing Program

AR 70–1
Army Acquisition Policy
AR 525–2
The Army Protection Program

Clarification of Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs
(Available at https://www.dote.osd.mil/.)

Committee on National Security Systems Instruction (CNSSI) 1253 Security Categorization and Control Selection for National Security Systems
(Available at http://www.disa.mil/.)

Director, Operational Test and Evaluation Memorandum, Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs
(Available at https://www.dote.osd.mil/.)

DOD CIO Memo, November 10, 2015, Subject: Outline and Guidance for Acquisition Programs' Cybersecurity Strategies
(Available at https://www.dau.mil/.)

DOD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle
(Available at https://www.dau.mil/.)

DOD 8570.01–M
Information Assurance Workforce Improvement Program
(Available at https://www.dtic.mil/.)

DODI 8581.01
Information Assurance (IA) Policy for Space Systems Used by the Department of Defense
(Available at https://www.esd.whs.mil/.)

Public Law 106–398
Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001
(Available at https://www.govinfo.gov/.)

40 USC Subtitle III
(Clinger-Cohen Act (CCA)) Information Technology Management
(Available at http://uscode.house.gov/.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (http://armypubs.army.mil); DD forms are available on the Office of the Executive Services Directorate website https://www.esd.whs.mil/.)

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B

Cybersecurity Strategy for Programs of Record Outline Template

B–1. Program information

a. Program name, Cybersecurity Strategy (Expectation 20–30 pages).
b. Date of last update.
c. Classification level.

B–2. 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. Use Table B–1 to list the 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 (for example, information system and platform information technology (PIT) system)).

c. System description. Describe the system being acquired and its intended operational environment, major system functions, subsystems, and so on.

Table B–1
Program Information Details

ACAT Level
Acquisition Life Cycle Phase
Current Milestone Decision and Date
Next Major Milestone and Date
Army Information Technology Registry Number & Acronym
Mission Designation (Mission Critical, Mission Essential, or Mission Support)
Type of System (Information Systems (Major Applications & Enclaves)); PIT (PIT Systems & PIT); IT Services internal & external); and IT products (software, hardware & applications)
Status of Department of Defense information networks (DODIN) connection: Program is connected to the DODIN, or Program is indirectly connected to DODIN, or Program is not connected to the DODIN
Security Objective: Confidentiality, Integrity, and Availability (C, I, & A) vs Impact Value (L, M, or H)

B–3. 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 in accordance with DODI 8510.01, CNSSI No. 1253, and NIST SP 800–60. Include expected list of information types and any planned or applicable overlays.

b. Initial control selection. Describe any planned deviations from the baseline security controls that are identified through the system categorization. Discuss how overlays are applied and discuss the process for determining inheritance and initial tailoring of security controls and other requirements, and ensure that they are reflected in the security plan. Update as the program progresses to reflect the current status and changes from previous strategy submission (that is, indicate AO approval of the security controls selection). Describe process for identifying security controls deemed "Not Applicable."

c. Joint Capabilities Integration and Development System specified requirements. Describe cyber survivability and cybersecurity requirements as defined in the initial capability document, capability development document and capability production document 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 (for example, communications security and cross-domain).

B–4. Cybersecurity approach (2 pages)

a. Management approach.

(1) *Stakeholder communication and documentation*. Describe methods and periodicity of communication between program and AO or AODR (in coordination with the AO), including the communication of risks and changes affecting risk posture. Describe how the program will plan for stakeholder input (for example, integrated product teams and working groups) and plan for assembly, dissemination, and coordination of required documentation including documentation of cybersecurity risks. Describe the process for AO or AODR (in coordination with the AO) 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 approach to attaining authorization for your system. List whether an automated tool (for example, 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. 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 test and evaluation (T&E) and operational T&E requirements trace to test plans (for example, T&E 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.

B–5. Cybersecurity implementation (5 pages)

a. Progress summary. See the Cybersecurity Strategy Progress Summary in the DOD CIO Memorandum dated 10 November 2015 to track and check-off completed activities (http://www.dau.mil/).

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) *Trusted systems and networks 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) *Risk management framework artifacts*. List status of RMF artifact implementation (for example, 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 events and status of development and approval since last milestone. List any criteria that were not met and describe a plan to address unmet criteria.

B–6. 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. Authorizing official or authorizing official designated representative (in coordination with the authorizing official) comments. AO/AODR provides comments on cybersecurity risk posture. Include date and approval status of RMF security plan and RMF authorization decision (if applicable).

B–7. Policy and guidance (less than a page)

List the primary policies and guidance employed by the program for preparing and executing the CSS and supporting activities, including both Office of the Secretary of Defense and component level policies and guidance.

B–8. Point(s) of contact (less than a page)

List responsible POCs and other stakeholders including name and contact information for the PO individuals responsible for the CSS document, PM, AO, and other relevant CSS stakeholders (for example, AODR, Security Control Assessor, Information System Security Manager, Chief Engineer, System Security Engineer).

B–9. 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 CSS.

B–10. Signature page (less than a page)

Include a signature page containing all individuals who have reviewed and approved the CSS, including the PM, AO, and Army CIO/G–6.

Glossary

Section I

Abbreviations

ACAT
acquisition categories

AO
authorizing official

AODR
authorizing official designated representative

AR
Army Regulation

CIO/G–6
Chief Information Officer/G–6

CNSSI
Committee on National Security Systems Instruction

CSS
Cybersecurity Strategy

DA
Department of the Army

DOD
Department of Defense

DODI
Department of Defense Instruction

DODIN
Department of Defense Information Network

DT&E
developmental test and evaluation

FDD
full deployment decision

FRP
full-rate production

FYDP
Future Years Defense Program

IA
information assurance

IT
information technology

KPP
key performance parameter

M&S
modeling and simulation

MDA
milestone decision authority

NIST
National Institute of Standards and Technology

PEO
program executive officer

PIT
platform information technology

PM
program Manager

PO
program office

POA&M
Plan of Action and Milestones

POC
points of contact

POR
Programs of Record

PPP
program protection plan

RFP
request for proposal

RMF
risk management framework

SAR
security assessment report

T&E
test and evaluation

TEMP
test and evaluation master plan

TSN
trusted systems and networks

USC
United States Code

Section II

Terms

Full deployment decision
Decision made by the MDA of a major automated information system acquisition program authorizing an increment of the program to deploy software for operational use

Full–rate production decision
The second effort part of the Production and Deployment phase as defined and established by DODI 5000.02 after low-rate initial production and following a successful full-rate production decision review.

Full–rate production decision review
MDA review to assess the results of initial operational test and evaluation and initial manufacturing and deployment to determine whether to approve proceeding to Full-Rate Production or Full Deployment.

Mission critical
A system whose operational effectiveness and operational suitability are essential to successful completion or to aggregate residual combat capability.

Mission essential
A system that meets the definition of “information system” in 40 USC (Clinger-Cohen Act), that the acquiring component head or designee determines it is basic and necessary for the accomplishment of the organizational mission.

Mission support
A system that focuses on the technical and business management approach for achieving program objectives and meeting customer requirements within specified resource constraints.

Program of record
Program as recorded in the current Future Years Defense Program (FYDP) or as updated from the last FYDP by approved program documentation (for example, acquisition program baseline, acquisition strategy, or Selected Acquisition Report).

Program protection plan
A risk-based, comprehensive, living plan to guide efforts for managing the risks to critical program information and mission-critical functions and components.

Section III

Special abbreviations and terms

This section contains no entries.