DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER (DON CIO)
CYBERSECURITY STRATEGY TEMPLATE
AND INSTRUCTIONS

MAY 2016

INTRODUCTION

1. Purpose:

The Cybersecurity Strategy (CSS) ensures compliance with the statutory requirements of the Clinger-Cohen Act (CCA), as implemented by Department of Defense (DoD) Instruction 5000.02, *Operation of the Defense Acquisition System*, and Secretary of the Navy (SECNAV) Instruction 5000.2E, *Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System.* The CSS must clearly describe the program's cybersecurity (CS) approach. Programs must update the CSS, as necessary, at each program milestone, program initiation for ships, full rate production (FRP), full deployment decision (FDD), and with major changes to the system.

2. CSS Format

Though not mandatory, this interim DON CSS template will certainly streamline and expedite the review by Department of Navy (DON) and DoD reviewers. The template provides guidance for format and content that will satisfy statutory review requirements. Programs must complete all sections of the template. If a section does not apply, justify that point in writing. If the program is in the early stages of development and the section is not applicable, or information required is not known at the time, state that point, indicating at what stage the information will be applicable or known. If a program cannot maintain functionality or cannot support one of the CS functions, then this failure becomes a shortfall and should be documented in the CSS. Citing other documents will not substitute for this essential information.

The enclosed template includes information from the current draft DoD CSS Outline; therefore, it is "interim" until the DoD outline is finalized and the cybersecurity enclosure for the DoD 5000 is completed.

3. Submission and Review

The DON Chief Information Officer (CIO) requires that the CSS be approved by the Program Manager and the Navy Echelon II or Marine Corps Major Subordinate Command Information Officer prior to formal submission to the DON CIO.

Submitters should plan for 60 days for DON CIO and DoD CIO review and approval of a CSS.

For Acquisition Category (ACAT) ID, IAC, and IAM programs, the DON CIO staff will coordinate the DoD review process. The Program Office representative may contact the DON CIO Cybersecurity & Infrastructure (CS&I) Team early to resolve questions or concerns about the CSS. Both the DON CIO and the DoD CIO CS staffs strongly encourage the Program Office to submit a draft CSS to the DON CIO for early informal review. The Program must provide a copy of the draft CSS to the respective Echelon II Command Information Officer (Command IO) at the same time they submit to the DON CIO for review. Additionally, the Program must keep the respective Command IO informed during the review process.

The Program Office must ensure that any material referenced in the CSS is readily available to the document/review chain on request. (i.e., Risk Management Framework, test, systems engineering, and requirements baseline documentation)

4. CSS Approval Process

The approval signature page of the CSS must include signatures from the Program Manager up through the appropriate Command Information Officer (see template sample page). The DON CIO signs only the CCA package as a whole, not the individual parts. The DON CIO does not sign the CSS separately.

The DON CIO CS&I Team reviews the CSS:

- Acquisition Category (ACAT) ID, IAC, and IAM programs at Milestone (MS) A, Development Request for Proposal (RFP) release decision, MS B, MS C, and Full Rate Production (FRP) / Full Deployment Decision (FDD): The DON CIO CS & I Director reviews the CSS and forwards it to DoD CIO for review. DON CIO CS&I staff coordinate with DoD CIO for reviews of the CSS. DoD CIO must review and approve the CSS prior to DON CIO's final approval of the CSS.
- ACAT IC and II programs: A CSS receives preliminary approval by the DON CIO CS&I Director.
- The DON CIO Director for CS&I forwards the CSS to the DON CIO CCA Coordinator, who incorporates it into the CCA Compliance Package for DON CIO signature. The DON CIO will keep the Program Office informed of CSS and CCA approval progress.

5. Interim CSS Template and Template Instructions

- All *red italic* content in the template indicates instructions or information required from the Program. As appropriate, the Program should replace or remove the instructions prior to submission.
- The target size of the CSS is 20-30 pages. The template recommends section lengths.
- For Official Use Only should be visible in the header and the footer of all pages; the Program/System name and version should also appear in the header (as shown in the template).
- **DoD CSS Evaluation Criteria:**
  - Evidence of comprehensive analysis (including System Security Engineering (SSE), Trusted Systems and Networks Analysis (TSN), 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.
  - Evidence of traceability between security controls and the baselines (functional, allocated, and product), and understanding of the balance between risks and requirements trades.
  - 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 for correct function or performance.
  - 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.
  - Evidence and understanding of ongoing risk management, including residual risks stemming from the failure to mitigate identified cybersecurity risks and vulnerabilities.
  - Within this guidance, the work "List" requires straightforward identification of information; the word "Describe" requires a brief description, often focused on the process; and the word "Discuss" means a more detailed narrative.

Cybersecurity Strategy
ACAT *XX*
FULL PROGRAM NAME (ACRONYM)
Increment or Phase
Version *XX (Strategy Version)*
DD MMM YYYY

LOGO (if desired)

Distribution authorized to the United States Department of Defense (DoD) and DoD staff and contractors only. Questions concerning technical content or any other requests for this document shall be referred to the *(include appropriate program name, and address).*

Warning: This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. Sec 2751 et seq.) or the Export Administration Act of 1979, as amended (Title 50 U.S.C. App. 2401 et seq.). Violators of these export laws are subject to severe criminal penalties. Dissemination of this document is controlled under DoD Directive 5230.25.

Handling and Destruction Notice: Comply with distribution statement and destroy by any method that will prevent disclosure of contents or reconstruction of the document.

This document contains information exempt from mandatory disclosure under the Freedom of Information Act (FOIA). Exemption 2 applies.

Table of Contents

Tables

Figures

I. Introduction *(3 pages)*

A. Executive Summary

Briefly describe the Program's cybersecurity strategy including the current status of the CS implementation. Include authors and contributors and their roles within the Program or organization.

B. Program Information

Table 1 - Program Information

Acquisition Category (ACAT) Level	ACAT *XX*
Acquisition Life Cycle Phase	*Phase*
Current Milestone Decision and Date	MS *X (YYYY MM DD)*
Next Major Milestone and Date	MS *X (YYYY MM DD)*
DITPR-DON ID Number & Acronym	*#####*
Authorization Tool System ID (i.e., eMASS system ID). If there are multiple instances of the tool, please identify the instance (e.g., SIPR, NIPR). If the system is not registered in a tool yet, please indicate the Future Tool.	*(XXXXX #####)* *Examples: USN SIPR eMASS 1111* *USMC MCCAST*
Mission Designation (Mission Critical, Mission Essential, or Mission Support)	Mission *X*
System Categorization – Confidentiality, Integrity, Availability (C-I-A)	Confidentiality - *(Low, Moderate, High)*, Integrity- *(Low, Moderate, High)*, Availability - *(Low, Moderate, High)*
Type of System (i.e., NSS, AIS Application, Enclave, Outsourced IT-Based Process, Platform IT (PIT) (PIT must include designation documentation) (**PIT Designation not required for Milestone A**)	*Type*
Status of Department of Defense Information Network (DoDIN) connection: Program is or is not connected to the DoDIN Please indicate DIRECT or INDIRECT Connection Indicators	*Connected / Not-Connected* to the DoDIN
Risk Management Process	*(RMF / DIACAP / XXX)*
Primary Network Connections	*Network*

C. System Description

1. Overview

Describe the mission, major system functions and sub-functions.

2. Operational Diagram

Provide a high level operational diagram.

Figure 1-Operational Diagram (OV-1)

3. System Diagram

Provide a system diagram including the authorization boundary, major elements, external connections and CONOPS summary.

Figure 2 - System Diagram

II. Sources of Cybersecurity Requirements ***(2-3 pages)***

A. System Categorization

Describe your approach to system categorization. Describe the participants in the effort by title, the role responsible for the final decision on categorization, rationale for the categorization, and indicate the categorization effort is compliant with the DoDI 8510.01 and CNSSI 1253. Identify planned or applicable overlays. Include a current or expected list of the information types supported by the system.

B. Initial Control Selection

Identify any system performance constraints that may cause substantial deviations from the baseline security controls and applicable overlays.

C. JCIDS Specified Requirements

Describe cyber survivability and cybersecurity requirements as defined in the Initial Capabilities Document (ICD), Capability Development Document (CDD), other Key Performance Parameters (KPP), Key System Attributes (KSA), or Additional Performance Attributes (APA). Should specifically state 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 DON/USMC/USN 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 stakeholders (AO, PM, SCA, Command Information Officer, etc.) including the communication of risks and changes affecting risk posture. Describe how the program will plan for stakeholder input (e.g., working groups including SE Working-level Integrated Product Team (WIPT)s, T&E WIPTs, Cybersecurity / IA WIPTs, SSE/Program Protection WIPTs, etc.) and plan for assembly, dissemination, and coordination of required documentation including documentation of cybersecurity risks. Describe the process for Authorization Official (or designee) review of the CS Strategy.

2. Acquisition of Cybersecurity Capabilities and Support

Describe the requirements you included or will include in your contract for cybersecurity, specifically regarding contractor functions. Add Contractor responsibilities, if any.

3. System Assessment and Authorization

a) Current approach

Please describe your current approach to attaining authorization for your system. Include milestones and schedule information with expected outcomes. Please indicate that you acknowledge that any authorization obtained as a result of legacy processes may be subject to a reduced authorization period.

b) Transition to Risk Management Framework

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

B. Technical Approach ***(5 pages)***

1. System Design and Architecture

Describe how you have integrated cybersecurity in to your system architecture and design. Describe your process for selecting and applying overlays, adding security controls, identifying compensating security controls, and identifying security controls as not applicable. Describe your approach to including stakeholders in the process and identify any supporting analysis you used to support cybersecurity decisions. Briefly describe how you capture and align the cybersecurity requirements in the Test and Evaluation Master Plan (TEMP), the Systems Engineering Plan (SEP), and the Cybersecurity Strategy (CSS).

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 & Evaluation (DT&E) and Operational Test & Evaluation (OT&E) requirements trace to test plans (e.g., Test and Evaluation Master Plan (TEMP), Security Assessment Plan). Include summary of requirements traceability of performance specifications to capabilities and attributes described in the governing documents.

3. Risk Assessment

List team members performing risk assessments by role. Describe plan for periodic RMF risk assessments (including periodicity and methodology); Describe how they will be integrated with other risk assessment activities, including Trusted System Network (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

A. Progress Summary – See Appendix A

Include the DoD Progress Summary Spreadsheet included as an appendix to this document.

B. Technical Implementation ***(5 pages)***

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. Do not repeat information described in section I.B. Include information relevant to the security architecture. 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 periodicity, stakeholders, and mechanisms for conducting ongoing cybersecurity 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 was 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 (TTP)s. 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. Include classified annexes as needed.

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. Describe how these risks are captured in the program risk register. Include failure to achieve thresholds and objectives in governing documents. This is more related to Program Risk – not directly related to system risk.

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 (AO)/Authorizing Official's Designated Representative (AODR) Comments

Please copy and complete the following table for each formal review of the CS Strategy to maintain historical information. Do not delete previous tables.

Table 2 - *Milestone X* AO/AODR Review

Milestone / Decision Point	
AO/AO Designee Name	
Authorization Date *(Indicate planned or achieved)*	
Authorization Status *(IATT, ATO/DATO/ATO w/Conditions)*	
Security Plan Review Date *(Date AO/AO Designee reviewed)*	
Security Plan AO/AO Designee Comments *(Include name of reviewer and approval status)*	

VI. Policy and Guidance ***(less than 1 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. If using the following partial list, please review to ensure the latest policy is referenced, as many are currently in the process of being updated.

- *DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015*
- *SECNAV Instruction 5000.2E, "Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System," September 1, 2011*
- *DoD Instruction 8500.01, "Cybersecurity," March 14, 2014*
- *DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014*
- *SECNAV Instruction 5239.3B, "Department of the Navy Information Assurance Policy," June 17, 2009*
- *DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015*
- *SECNAV Instruction 5239.20, Department of the Navy Cybersecurity/Information Assurance Workforce Management, Oversight, And Compliance," June 17, 2010*
- *CNSS Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, " June 10, 2013*
- *CNSSI No 1253, Security Categorization and Control Selection for National Security Systems, 27 March 2014*

VII. Points of Contact ***(less than 1 page)***

Table 3 - Points of Contact(s)

Role	Name	Phone	Email
Program Manager (SES/GO/FO)			
Command Information Officer (CIO)			
User Representative			
Information System Security Manager (ISSM)			
Information System Security Engineer			
Authorizing Official			
Authorizing Official Designated Representative			
Security Control Assessor			
Validator			
Additional Roles			

Additional Roles			
Additional Roles			
***Indicates the POC for the DON CIO staff to contact with concerns or questions regarding the CS Strategy** *(please mark the appropriate POC with an asterisk)*			

VIII. Other Considerations *(less than 1 page)*

Please indicate additional considerations including approved waivers, special considerations or alternate process agreements (with stakeholders and any special arrangements). Document any agreements with DON organizations, DON CIO or the Services related to the Cybersecurity Strategy.

IX. Signature Page

This Cybersecurity Strategy has been reviewed and approved by:

______________________________	__________
Program Manager	Date
______________________________	__________
FO/GO/SES Sponsor	Date
______________________________	__________
Command Information Officer	Date
______________________________	__________
{Additional Endorsement}	Date

APPENDIX A - 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*	

Program/System Name, Version **Cybersecurity Strategy Progress Summary** *YY-MMM-DD*

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
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	
System registered			DoDI 8510.01	
Security Plan approved by AO/AODR			DoDI 8510.01	
Continuous Monitoring Strategy approved by AO/AODR			DoDI 8510.01	

Program/System Name, Version **Cybersecurity Strategy Progress Summary** ***YY-MMM-DD***

Cybersecurity Integration Activity	**YES**	**NO**	**Reference**	**Comments / Remarks**
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)	

Program/System Name, Version **Cybersecurity Strategy Progress Summary** *YY-MMM-DD*

Cybersecurity Integration Activity	**YES**	**NO**	**Reference**	**Comments / Remarks**
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	
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**	

Program/System Name, Version **Cybersecurity Strategy Progress Summary** *YY-MMM-DD*

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
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)	

Program/System Name, Version **Cybersecurity Strategy Progress Summary** *YY-MMM-DD*

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
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	
Milestone C			**Reference: DoDI 5000.02**	
Milestone C Exit Criteria Approved			DoDI 5000.02	
Network connection approval package submitted			DoDI 8510.01	

Program/System Name, Version **Cybersecurity Strategy Progress Summary** *YY-MMM-DD*

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
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	

Program/System Name, Version **Cybersecurity Strategy Progress Summary** ***YY-MMM-DD***

Cybersecurity Integration Activity	**YES**	**NO**	**Reference**	**Comments / Remarks**
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	
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	

Program/System Name, Version **Cybersecurity Strategy Progress Summary** ***YY-MMM-DD***

Cybersecurity Integration Activity	YES	NO	Reference	Comments / Remarks
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