CYBERSECURITY STRATEGY
OUTLINE and GUIDANCE

Version 1.3
August 2020



Department of Defense
Chief Information Officer
Cybersecurity Risk Management

CYBERSECURITY STRATEGY GUIDANCE

1. This document provides an outline and high-level guidance on the expectations for the Cybersecurity Strategy (CSS), previously identified as the Information Assurance Strategy, primarily included as an appendix to a system’s Program Protection Plan, as required by the Clinger-Cohen Act (40 U.S.C. Subtitle III) in the 2001 NDAA §811(P.L. 106-398) and DoDI 5000.02, *Operation of the Defense Acquisition System.* USD for Acquisition and Sustainment (A&S) introduced the Adaptive Acquisition Framework (AAF) to the Defense Acquisition System in 2019. This led to a complete revision of the DoDI 5000.02; and the redesignation of “functional” enclosures as DoD instructions; including Enclosure 11, *Requirements Applicable to All Programs Containing Information Technology (IT),* and Enclosure 14, *Cybersecurity in the Defense Acquisition System*. DCIO-CS coordinated current CSS updates with USD A&S, and USD R&E.

Additional related policies and guidance include:

DoDI 8500.01 – *Cybersecurity*

DoDI 8510.01 – *Risk Management Framework (RMF) for DoD Information Technology (IT)*

*DoDI 8580.01 –Information Assurance (IA) in the Defense Acquisition System*

*DoDI 8330.01 --* Interoperability of Information Technology (IT), Including National Security Systems (NSS)

DoDI 8530.01 – *Cybersecurity Activities Support to DoD Information Network Operations*

DoDI 5200.44 – *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*

NIST SP 800-53 Rev. 4 – *Security and Privacy Controls for Federal Information Systems and Organizations*

NIST SP 800-82 Rev. 2 – *Guide to Industrial Control Systems (ICS) Security*

NIST SP 800-160 Vol. 1 and Vol. 2 – *Systems Security Engineering*

NIST SP 800-161 – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*

1. **CSS scope and lifecycle.** The CSS outlines plans for, and implementation status of, projected cybersecurity activities across all phases of a system’s lifecycle. The CSS is applicable to all Adaptive Acquisition Framework (AAF) pathways, and retains operational relevance beyond Milestone decisions into system sustainment. The PMO must maintain and update the CSS across the acquisition lifecycle. The PMO shall update the CSS when planning for software and hardware updates; mitigations to emerging threats, or changes in Portfolio risk tolerances. or Risks may emerge as threats evolve, and the impacts of discovered or existing vulnerabilities or exposures may cause risk at any time, the program office and the system owner will actively review, update, employ, and maintain the CSS for the life of the system.
2. **Requirements.** An initial draft of a system’s CSS is drawn from the JCIDS Gap Assessment, Initial Capabilities Document, capabilities need statements, initial Mission-based Cyber Risk Assessment (MBCRA), Cyber Survivability Attributes (CSA), and Operations Concept during the Material Solution Analysis phase of the system acquisition lifecycle.
3. **Acquisition.** The CSS is a required acquisition program document created and maintained by the Program Office and appended to the Program Protection Plan (PPP). The Program Office initially develops the CSS for Milestone A, and updates and maintains it as the program evolves. The CSS describes the program’s planned implementation of the system’s required cybersecurity protections throughout the acquisition lifecycle. The program office will review, update, and seek approval for the CSS to inform key program milestone decisions and during Operations and Sustainment in partnership with the system owner.
4. **Cybersecurity Test and Evaluation (T&E).** Cybersecurity T&E events verify and validate system security engineering practices and sufficiency of implemented cybersecurity requirements and controls (traced to CSAs). T&E events are a means for friendly discovery of areas needing remediation for resilience. Cybersecurity T&E informs decision authorities and Authorizing Officials (AOs) of cybersecurity risks to mission execution. The CSS’s description of the testing continuum and the system’s expected operational context must remain consistent with that of the Test and Evaluation Master Plan (TEMP), to ensure that the system is prepared for and tested under the cyber-contested environmental conditions it will face in operations. See the DOT&E *TEMP Guidebook 3.1*, its Appendix E, and *DoD Cybersecurity Test and Evaluation Guidebook*.
5. **Authorizations to Operate.** The system’s AO reviews the progress of CSS implementation at key program milestones to ensure that upon successful completion of testing the system will meet all criteria necessary for authorization to operate.
6. **Cyber Defense in Operations and Sustainment.** Once deployed, a system’s owners and operators must maintain and update the system’s cybersecurity posture to reflect changes in mission environments. System owners should plan for recurring testing at a cadence informed by the MBCRA. T&E events should support assessment of system cyber survivability and operational resilience. Cybersecurity Service Providers (CSSPs) must adapt to evolving threats and maintain operating environments, and system configurations, as threats evolve. CSSPs must provide command and control of Cyber Defenses and account for system dependencies needed to achieve mission critical and essential tasks. For example, a system may need to join different networks or connect with systems other than those initially planned.
7. The CSS consolidates elements of various program initiatives and activities relating to cybersecurity planning, T&E, implementation, and lifecycle risk management. Use of existing analysis and documentation is strongly encouraged where practical to support development of the CSS. Any referenced information must be made available for document reviews. References may include requirements baselines, architecture and systems engineering plans, MBCRA results, test plans and results, RMF documentation, Orders, and Plans of Action and Milestones (POA&Ms) to maintain system cybersecurity. Append classified annexes as needed to provide accurate information.
8. Authors 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:
9. Consideration of the expected level of threat and the intended system Concept of Operations (CONOPS), operating environment, and operations tempo.
10. Consideration of mission essential and mission critical tasks the system supports directly or indirectly.
11. Evidence of comprehensive analysis, including System Security Engineering (SSE), Trusted Systems and Networks (TSN), MBCRA results, and system survivability and threat modeling to support the planning and implementation of system cybersecurity.
12. For systems in acquisition – Evidence of implementing cybersecurity, system survivability and resilience requirements throughout the design, engineering, and production stages of the acquisition lifecycle. Include traceability of requirements to system baselines (functional, allocated, and product) and security controls, and demonstrate the balance between risks and engineering trades.
13. For systems in operations and sustainment – Evidence of maintaining and enhancing cybersecurity, survivability, and resilience as missions, threats, and operational contexts evolve over the system’s lifespan.
14. 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.
15. Ensuring cybersecurity requirements are testable and measurable, planning for cybersecurity, cyber survivability, and operational resilience test and evaluation throughout the acquisition lifecycle, and testing RMF security controls. See the DOT&E *TEMP Guidebook 3.1*, its Appendix E, and *DoD Cybersecurity Test and Evaluation Guidebook*.
16. Evidence and understanding of ongoing risk management, including residual risks stemming from the failure to mitigate identified cybersecurity risks and vulnerabilities.
17. Authors should utilize the following outline and the above principles in the preparation of their CSS documentation. Document updates throughout the lifecycle should emphasize accomplishments as well as changes from previous Strategy submittals. 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 counts. Specifically, where sections ask for documentation to “list”, “describe”, “discuss”, or summarize 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;
* “Summarize” requires a brief description covering a broad scope.

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 CSS to inform CIO review and approval. For additional guidance on content, resources, and references for the CSS, refer to the RMF Knowledge Service (<https://rmfks.osd.mil>).

CYBERSECURITY STRATEGY OUTLINE

*(PROGRAM NAME)* Cybersecurity Strategy *(Expectation: 20-30 pages)*

 *Version and date*

 *Approval signatures*

1. Introduction: *(3 pages)*
2. Executive Summary – *Summarize the system’s overall CSS, identify authors and contributors, and characterize implementation status.*
3. Program Information – *List the Acquisition Category (ACAT) level of the program, current phase within the Adaptive Acquisition Framework, next major milestone decision and date, and any other relevant cybersecurity program information such as system type determination (e.g. Information System, Platform IT (PIT) System).*
4. System Description – *Describe the system (as planned or as built) and its intended operational environment, map mission essential system functions, subsystems, external interfaces, critical mission data flow to functions and architecture, etc. Depict or describe the mapping of mission essential functions and critical mission data flows to system functions and system architectures.*
5. Threat Characterization – *Describe the system’s exposure to expected levels of threat throughout its lifespan to include program office, developer, and other supply chain exposures.*
6. Sources of Cybersecurity Requirements: *(2 pages)*
7. JCIDS Specified Requirements – *Summarize cyber survivability and cybersecurity requirements as defined in the Initial Capability Document (ICD) or Capability Development Document (CDD), as part of the System Survivability Key Performance Parameter (KPP), or other cybersecurity capability requirements defined by any other KPPs, key system attributes, or additional performance attributes. List the system’s Mission Type, Adversary Threat Tier, Cyber Dependency Level, Impact Level of System Compromise, and overall Cyber Survivability Risk Category.*
8. CNSSI, DoD, and NIST Requirements
	1. System Categorization – *Describe the approach for completing system categorization, including who is involved and responsible, rationale, and results of system categorization, in accordance with DoDI 8510.01 and CNSSI 1253. Include lists of information types and any planned or applicable overlays.*
	2. Initial Control Selection – *Identify expected sets of cybersecurity controls. Describe major system performance constraints that may result in substantial deviations from established baseline control sets or applicable overlays. Describe the process for identifying security controls deemed “Not Applicable”.*
9. Other Requirements – *Describe any additional cybersecurity requirements from other sources such as organization, Service-level, system functional requirements, or new operational requirements (e.g., CSAs, COMSEC, Cross-Domain).*
10. Management Approach: *(4 pages)*
11. Stakeholder Communication and Documentation – *Describe methods and periodicity of communication between program and stakeholders. Describe plans for stakeholder input (e.g., Integrated Product Teams (IPT), working groups) and for assembly, dissemination, and coordination of required documentation including documentation of cybersecurity risks and any changes affecting risk posture. Describe the process for AO (or designee) review of the CSS.*
12. System Engineering Management – *Summarize the system engineering management processes for monitoring and controlling the system development program.*
13. Acquisition of Cybersecurity Capabilities and Support – *Describe the methods to incorporate cybersecurity requirements and developer responsibilities into contract statements of work. Identify cybersecurity support services necessary for operations such as CSSPs.*
14. Cybersecurity Engineering – *Describe the process used to ensure implementation of cybersecurity, system survivability and operational resilience requirements throughout the design, engineering, and production lifecycle (e.g., CSAs, design practices, engineering reviews, and developmental testing efforts). Describe requirements tracing requirements to engineering baselines, and how requirements and engineering solutions trace to developmental and operational test plans. Include the engineering efforts to implement and test/assess program protection plans and critical program information, critical components, and critical functions.*
15. Risk Management – *Describe the processes for identifying and exposing cybersecurity risks, including supply chain risks. Describe the plan for periodic risk assessments. Describe the plan for incorporating mitigations into engineering efforts or translating into compensating operational tactics, techniques, and procedures.*
16. Developmental, Operational, and Integrated Testing – *Describe the processes of assessing cybersecurity, cyber survivability risk posture, and operational resilience using a continuum of cooperative vulnerability, and adversarial cyber test and evaluation events. Describe the planned/implemented prioritization, remediation, mitigation, and verification of corrective action processes for identified vulnerabilities and risks.*
17. System Assessment and Authorization – *Describe the approach to attaining authorizations to connect and operate the system. List the automated tools used (e.g., eMASS). List key role assignments. Describe the authorization boundary. Include milestones and schedule information with expected outcomes.*
18. Operations Management – *Describe how cybersecurity will be managed in system operations and sustainment; for example, by establishing a Security Operations Center to monitor the system’s security status or contracting with a CSSP. Identify means for auditing service provider performance and incident response activities.*
19. Technical Approach: *(5 pages)*
20. System Design and Architecture – *Describe the high-level plan to integrate cybersecurity, survivability, and resilience requirements into the system’s architecture and design. Discuss the processes for identifying and applying control overlays, for identifying which controls will be provided by other systems, and for any other initial tailoring activities. Describe stakeholder involvement and any supporting analysis. Understand responsibilities to provide cybersecurity command and control elements.*
21. Requirements Traceability – *Describe the process and mechanisms used to ensure that requirements (to include specified, implied, and essential) are traceable to system baselines (functional, allocated, and product) and to security controls throughout the system lifecycle. Describe the tracing of all cybersecurity, survivability, and resilience requirements to test plans (e.g., Test and Evaluation Master Plan, Test and Evaluation Strategy, Security Assessment Plan, Lifecycle Sustainment Plan).*
22. Risk Assessments – *Describe processes for periodic MBCRAs (including periodicity, stakeholders, and methodology). Describe the integration of MBCRA recommendations with other risk assessment activities, including TSN Criticality Analysis and programmatic and operational risk assessments to inform prioritization and tradeoff decisions.*
23. External Connections – *List external connections, including temporary, to other systems and infrastructure, and describe the approach to protecting system interfaces and exchanged data to include the incident response (recovery) approach after compromise of one of more interfaces. Discuss potential risks or vulnerabilities inherited or introduced by external systems or infrastructure and their interfaces. Identify dependencies on other external systems and interfaces with those systems, and their authorization status.*
24. Inherited Protection – *List inherited or CSSP security functions outside the program or other sources. Plan to test and evaluate the effectiveness of the protections.*
25. Review Processes – *Describe how entry and exit criteria for Systems Engineering Technical Review (SETR) events will be established. Describe any significant changes to the planned technical approach.*
26. Test and Evaluation – *Describe planned developmental, operational, and sustainment cybersecurity testing to include verifying and validating effectiveness of implemented cybersecurity requirements, controls, inherited risks (including developer environment, processes, automated tools, supply chain, interfaces) and protections (including CSSPs, program protections, and inherited defensive functions), cyber survivability risk posture and operational resilience.*
27. Implementation Progress: *(4 pages)*

*Describe the progress made in implementing cybersecurity and system survivability requirements.*

1. System Design and Architecture – *Describe the implementation status of the overall system design and architecture. Describe any significant 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. Security Architecture – *Describe the implementation status of the security architecture.*
3. Criticality Analysis – *Describe results of or updates to the TSN Criticality Analysis. Include mission decomposition.*
4. Requirements Traceability – *Describe the status of allocation of mission essential functions to system functionality as well as the allocation of security functions to system baselines. Summarize the traceability of requirements to system design components.*
5. Engineering and Manufacturing – *Describe the status of engineering and manufacturing to meet security and survivability requirements. (e.g., status of control implementation and indications of effectiveness from developmental testing).*
6. Test and Evaluation – *Describe the results of developmental, operational, and integrated cybersecurity, survivability and resilience testing. These results should include an assessment of the effectiveness of the system to continue to operate despite a cyber-event, not just that the security controls are in place.*
7. Test Completion Status – *Summarize the progress of cybersecurity developmental and operational testing..*
8. RMF Compliance – *Summarize the results of RMF security controls testing.*
9. Cyber Survivability Risk Posture and Operational Resilience – *Summarize the assessment of the controls, security engineering requirements, defensive capabilities, remediation actions, and mitigations in meeting mission requirements.*
10. Operation and Sustainment – *Describe the status of maintaining system configuration, installing updates and patches, and ongoing testing.*
11. Other – *Describe any other cybersecurity implementation considerations.*
12. Operation and Sustainment: *(4 pages)*

*Describe the defensive cyber operations necessary to support system operations.*

1. Threat assessments – *Describe the threat assessments and update schedules necessary to support cyber defenses. Assessments should exercise the cyber defensive command and control of data, paths, equipment, and dependencies enabling mission critical and essential tasks.*
2. Vulnerability management – *Summarize the approach to vulnerability management (plans of action, milestones, status reporting).*
3. Vulnerability assessments and analysis – *Describe the techniques used to assess and analyze system vulnerabilities (e.g., network discovery, vulnerability scanning, static code analysis, penetration testing).*
4. Remediation and Mitigation Plan – *Describe the remediation actions, mitigations, verification of the effectiveness through tests of the remediation and mitigation, and plans for ongoing identification and evaluation of risk to mission from new or existing vulnerabilities and threats.*
5. Sustainment Test and Evaluation – *Describe the results of sustainment cybersecurity, survivability and resilience testing. These results should include an assessment of the effectiveness of the system to continue to operate despite a cyber-attack and the other in place sustainment capabilities in this section.*
6. System monitoring – Describe the techniques used to monitor system operations.

Malware detection and protection – *Describe the techniques used to detect and remove malware.*

1. Continuous monitoring – *Describe the techniques used to monitor system operations on a continuous basis.*
2. Insider threat user activity monitoring – *Describe the techniques used to detect and block unauthorized system activity.*
3. Cyber incident handling – *Summarize the system incident handling procedures, responsible parties, and reporting channels.*
4. Attack sensing and warning – *Describe the available sources of cyber attack warnings, as well as any responsibilities for detecting attacks and issuing warnings for other systems.*
5. Command and Control – *Describe the ability to provide command and control over mission critical paths, data, and equipment.*
6. 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 OSD and Component-level policies and guidance.*
7. Point of Contact(s): *(Less than a page)* *List responsible POC and other stakeholders including name and contact information for individuals responsible for the CSS* *document and other relevant CSS* *stakeholders (e.g. Program Manager, Authorizing Official, Information System Security Manager, Chief Engineer, System Security Engineer, Security Control Assessor, Developmental and Operational Cyber Test Organizations).*
8. Other considerations: *(Less than a page)* *Identify additional considerations 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.*
9. Signature Page: *(Less than a page) Include a signature page containing all individuals who have reviewed and approved the CSS (e.g., Program Manager, Authorizing Official, cognizant CIO/G6, Department or Service Acquisition Executive).*