



National Security Agency/Central Support Service



INFORMATION ASSURANCE DIRECTORATE

CGS Development Capability

Version 1.1.1

Development is the creation of a solution based on an identified need. The development phase of the lifecycle comprises many activities that ensure that information assurance (IA) is included from concept up to the Deployment Capability. The Development Capability includes the incorporation of IA during architecture, concept, design, implementation/build, integration, requirements, and test.

07/30/2012



CGS Development Capability

Version 1.1.1



Table of Contents

1	Revisions	2
2	Capability Definition	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions	5
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations	6
7	Capability Interrelationships.....	8
7.1	Required Interrelationships	8
7.2	Core Interrelationships	9
7.3	Supporting Interrelationships.....	10
8	Security Controls	10
9	Directives, Policies, and Standards	14
10	Cost Considerations	19
11	Guidance Statements.....	20



CGS Development Capability

Version 1.1.1



1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



CGS Development Capability

Version 1.1.1



2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Development is the creation of a solution based on an identified need. The development phase of the lifecycle comprises many activities that ensure that information assurance (IA) is included from concept up to the Deployment Capability. The Development Capability includes the incorporation of IA during architecture, concept, design, implementation/build, integration, requirements, and test.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Development Capability focuses on the incorporation of IA throughout the development phase of the lifecycle. The Capability depends on coordinating relationships between systems security engineers (SSEs), stakeholders, accrediting authorities, developers, and test teams to meet development IA objectives. The Development Capability shall employ services from a program management role or office to ensure that all activities and resources are managed according to the program management plan and are able to meet the IA objectives established. This shall also provide visibility into the development activity to other programs with dependencies on the development activity.

The Development Capability includes the use of development processes that are established and approved in the IA Policies, Procedures, and Standards Capability. The Development Capability encompasses requirements development, requirements management, and verification and validation (made up of penetration testing, security testing, code review, and architecture reviews). Prior to beginning requirements definition in the Development Capability, a Concept of Operations (CONOPS) shall be defined. This CONOPS shall align with current standards and be documented and approved by the stakeholders.



CGS Development Capability



Version 1.1.1

Requirements development occurs throughout the development of the solution. It begins with the solution concept, which is decomposed to define the requirements for the system. During concept decomposition, security requirements shall be defined and be traced back to the solution architecture. Requirements development also relies on the definition of the Enterprise architecture, which will provide insight into requisite requirements. Requirements shall be simple, measurable, achievable, realistic, and testable (SMART). In addition, as a part of requirements development, certification and accreditation (C&A) requirements shall be incorporated, along with interface interoperability and performance requirements.

As the development activity progresses, requirements evolve and mature to maintain alignment with the logical and physical architecture. The requirements management process shall update and maintain the defined security requirements. As they are updated, traceability of requirements to the architecture shall be maintained and documented. Documentation (e.g., the requirements traceability matrix) shall align the requirements with the components and interfaces as part of the requirements decomposition, in accordance with the logical and physical architectures.

The developed solution's required level of assurance (confidence that the security is effectively implemented) shall be established before verifications and validations are performed. Penetration testing, security testing, code review, and architecture review objectives shall be defined in accordance with the required assurance. These validations shall occur throughout the development including the various stages of product integration.

Security code reviews and architecture reviews shall be conducted against incremental builds. Code reviews shall be automated, and all reviews shall be performed using accepted industry standards, such as Unified Modeling Language (UML). Architecture reviews are provided in accordance with the Architecture Reviews Capability.

Development testing shall include functional and security testing, which shall be conducted in a mock operational environment that is consistent with the Enterprise's operational environment. Applications and products shall be tested on platforms different from the platforms on which they were developed. Penetration testing (provided through the Network Security Evaluation Capability) shall be performed against the solution during development. Testing shall be as automated as possible and be performed by independent testers who understand the requirements, which shall be provided by the SSEs. The test plans and results shall be documented and stored in a central repository



CGS Development Capability



Version 1.1.1

for future use. The test objectives shall trace to the requirements, which trace to the solution components. In addition, test findings shall be shared with the development team and stakeholders.

The Development Capability includes coordination of security expertise and collaboration with the SSEs who will ensure the C&A (see Risk Analysis Capability) and security requirements are defined along with the functional requirements. The SSEs shall also ensure that the development team provides a solution that considers usability and maintainability of the security during the operations and maintenance phase of the lifecycle. The C&A and security requirements shall be understood, vetted, and accepted by the developers, independent testers, accrediting authority, and security stakeholders.

All activities performed within the Development Capability (e.g., architecture, concept, design, implementation/build, integration, requirements, and test) shall be documented according to industry standards and procedures (see the IA Policies, Procedures, and Standards Capability). In addition, peer and stakeholder milestone reviews shall be incorporated at each development activity stage. These periodic milestone reviews (as defined by the development schedule) shall include all stakeholders and shall have requirements acceptance prior to moving into next stage of development. For example, milestone reviews shall include a system requirements review and acceptance after the requirements have been defined prior to moving into the architecture and design stages of development. Other examples include preliminary and critical design reviews.

This Capability shall cover the Configuration Management of documentation created during the development phase. The documentation shall be developed and maintained along with the solution development. Documentation shall include product information along with required C&A documentation. Documentation shall follow versioning and control as defined by Configuration Management practices. Configuration management of the security solution and code during development is covered within the Configuration Management Capability.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. The Organization has selected and documented a development process.



CGS Development Capability

Version 1.1.1



2. The Organization has defined and documented the Enterprise architecture.
3. The defined need/capability and a CONOPS produced have been vetted and approved.
4. The resources for solution development have been provided.
5. Policies have been defined for execution of the development process.
6. All programs have an established program management role or office to manage activities and resources.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability manages a secure code repository.
2. The Capability fully tests solutions prior to deployment.
3. The Capability establishes a review process that includes quality assurance.
4. The Capability provides development for revisions to developed products.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When the Development Capability is implemented correctly, the Organization will possess a process for efficiently and effectively incorporating security throughout the development stages from the original solution concept to the development of the functionality that supports the Enterprise mission needs. An Organization will use approved and established processes, which include requirements development, requirements management, and verification and validation (made up of penetration testing, security testing, code reviews, and architecture reviews). Approved processes are defined in the IA Policies, Procedures, and Standards Capability for the Development Capability.

An Organization will ensure that the requirements are derived and decomposed according to the defined concept. Requirements will be defined according to the SMART principles, and the requirements will be traceable back to the defined need.



CGS Development Capability

Version 1.1.1



Once the requirements have been developed, an Organization will effectively and efficiently manage its requirements by updating the requirements throughout the development and maintaining traceability of defined security requirements to the logical and physical architectures. The Organization will ensure C&A (see Risk Analysis capability) and security requirements, along with the functional (including use and maintenance of security functions and protections) requirements, are understood, vetted, and approved by the development team and stakeholders.

An Organization will provide independent verification and validation of the developed solution within the Development Capability. Verification and validation includes testing and code and architecture reviews. The Organization will employ independent testing teams and ensure that testing is performed in a segregated environment that mimics the Organization's operational needs. The Network Security Evaluations Capability will provide penetration testing. Within the Organization, all products that are a part of the Development Capability will go through a thorough functional and security testing process. This testing will be as automated as possible and will be conducted by independent testers. During execution of the Development Capability and prior to deployment, test findings will be shared with the development team (e.g., SSEs, stakeholders, developers, and accrediting authorities) and stored in a central repository. An Organization will conduct automated security code reviews and architecture reviews against incremental builds using accepted industry standards. These reviews will provide quality assurance for the Capability.

Organization's SSEs will be responsible for ensuring that IA is integrated through all development activities (e.g., architecture, concept, design, implementation/build, integration, requirements, and test). In addition, the SSEs will communicate with stakeholders, accrediting authorities, developers, and independent testers to ensure that security concepts are implemented within the Development Capability.

An Organization will establish the appropriate approval processes and ensure that those processes are implemented and used throughout the Capability. The approval processes shall be incorporated at key milestones during development before progressing to the next phase. An Organization will provide the required security and C&A documentation, along with the solution, so that the appropriate risk decision can be made. Security stakeholders will provide approval.



CGS Development Capability

Version 1.1.1



7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping-The Development Capability relies on the Network Mapping Capability to provide information about the current operating environment, which is considered during the development of requirements.
- Network Boundary and Interfaces-The Development Capability relies on the Network Boundary and Interfaces Capability to provide information about the current operating environment, which is considered during the development of requirements.
- Utilization and Performance Management-The Development Capability relies on the Utilization and Performance Management Capability to provide information about utilization and performance targets and baselines, which are considered during the development of requirements.
- Understand Mission Flows-The Development Capability relies on the Understand Mission Flows Capability to provide mission flow information, which is considered during the development of requirements.
- Understand Data Flows-The Development Capability relies on the Understand Data Flows Capability to provide data flow information, which is considered during the development of requirements.
- Hardware Device Inventory-The Development Capability relies on the Hardware Device Inventory Capability to provide information about the current operating environment, which is considered during the development of requirements.
- Software Inventory-The Development Capability relies on the Software Inventory Capability to provide information about the current operating environment, which is considered during the development of requirements.
- Understand the Physical Environment-The Development Capability relies on the Understand the Physical Environment Capability to provide information about the current operating environment, which is considered during the development of requirements.



CGS Development Capability



Version 1.1.1

- Configuration Management-The Development Capability relies on the Configuration Management Capability to provide configuration management services for a developed solution and code.
- Architecture Reviews-The Development Capability relies on the Architecture Reviews Capability to conduct architecture reviews during the development phase of the lifecycle to ensure that the architecture meets requirements during system design.
- Physical Hunting-The Development Capability relies on the Physical Hunting Capability to provide TEMPEST inspections for systems under development.
- Contingency Planning-The Development Capability relies on the Contingency Planning Capability to provide information about contingency plans, which will feed into requirements.
- Risk Analysis-The Development Capability relies on the Risk Analysis Capability to provide information about the acceptable level of Enterprise risk, which contributes to the development of system requirements.
- Risk Mitigation-The Development Capability relies on the Risk Mitigation Capability to provide mitigation information, which is used to define security requirements for the solution being developed.
- Finance-The Development Capability relies on the Finance Capability to provide funding, including C&A funding, throughout the development lifecycle.
- Acquisition-The Development Capability relies on the Acquisition Capability to provide supply chain risk management services when components need to be purchased for the solution being developed.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management-The Development Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards-The Development Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness-The Development Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.



CGS Development Capability



Version 1.1.1

- IA Training-The Development Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities-The Development Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Security Evaluations-The Development Capability relies on the Network Security Evaluations Capability to conduct assessments on systems while they are still under development.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
CM-4 SECURITY IMPACT ANALYSIS	Enhancement/s: (1) The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. (2) The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements of the system.
PL-2 SYSTEM SECURITY PLAN	Control: The organization: a. Develops a security plan for the information system that: Is consistent with the organization's enterprise architecture; Explicitly defines the authorization boundary for the system;



CGS Development Capability



Version 1.1.1

	<p>Describes the operational context of the information system in terms of missions and business processes;</p> <p>Provides the security category and impact level of the information system including supporting rationale;</p> <p>Describes the operational environment for the information system;</p> <p>Describes relationships with or connections to other information systems;</p> <p>Provides an overview of the security requirements for the system;</p> <p>Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and</p> <p>Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;</p> <p>b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.</p> <p>Enhancement/s:</p> <p>(1) The organization:</p> <p>(a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and</p> <p>(b) Reviews and updates the CONOPS [Assignment: organization-defined frequency].</p> <p>Enhancement Supplemental Guidance: The security CONOPS may be included in the security plan for the information system.</p> <p>(2) The organization develops a functional architecture for the information system that identifies and maintains:</p> <p>(a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;</p> <p>(b) User roles and the access privileges assigned to each role;</p>
--	--



CGS Development Capability



Version 1.1.1

	<p>(c) Unique security requirements;</p> <p>(d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and</p> <p>(e) Restoration priority of information or information system services.</p>
<p>PM-11 <i>MISSION/BUSINESS PROCESS DEFINITION</i></p>	<p>Control: The organization:</p> <p>b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.</p> <p>Enhancement/s: None Specified</p>
<p>SA-3 <i>LIFE CYCLE SUPPORT</i></p>	<p>Control: The organization:</p> <p>a. Manages the information system using a system development life cycle methodology that includes information security considerations;</p> <p>b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and</p> <p>c. Identifies individuals having information system security roles and responsibilities.</p> <p>Enhancement/s: None Specified.</p>
<p>SA-8 <i>SECURITY ENGINEERING PRINCIPLES</i></p>	<p>Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.</p> <p>Enhancement/s: None Specified</p>
<p>SA-10 <i>DEVELOPER CONFIGURATION MANAGEMENT</i></p>	<p>Control: The organization requires that information system developers/integrators:</p> <p>a. Perform configuration management during information system design, development, implementation, and operation;</p> <p>b. Manage and control changes to the information system;</p> <p>c. Implement only organization-approved changes;</p> <p>d. Document approved changes to the information system; and</p> <p>e. Track security flaws and flaw resolution.</p> <p>Enhancement/s:</p> <p>(1) The organization requires that information system developers/integrators provide an integrity check of software to</p>



CGS Development Capability



Version 1.1.1

	<p>facilitate organizational verification of software integrity after delivery.</p> <p>(2) The organization provides an alternative configuration management process with organizational personnel in the absence of dedicated developer/integrator configuration management team.</p> <p>Enhancement/s: None Specified</p>
<p>SA-11 DEVELOPER SECURITY TESTING</p>	<p>Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):</p> <ul style="list-style-type: none"> a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes. <p>Enhancement/s:</p> <p>(1) The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.</p> <p>(2) The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.</p> <p>(3) The organization requires that information system developers/integrators create a security test and evaluation plan and implement the plan under the witness of an independent verification and validation agent.</p>
<p>SC-18 MOBILE CODE</p>	<p>Enhancement/s 2:</p> <p>(2) The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [Assignment: organization-defined mobile code requirements].</p>
<p>SC-31 COVERT CHANNEL ANALYSIS</p>	<p>Control: The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.</p>



CGS Development Capability



Version 1.1.1

	<p>Enhancement/s:</p> <p>(1) The organization tests a subset of the vendor-identified covert channel avenues to determine if they are exploitable.</p>
<p>PM-8 <i>CRITICAL INFRASTRUCTURE PLAN</i></p>	<p>Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.</p> <p>Enhancement/s: None Specified</p>

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Development Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 801, Acquisition, 16 August 2009, Unclassified	Summary: National Intelligence Program (NIP) major system acquisitions (MSA) shall use the acquisition process model identified in Intelligence Community (IC) Policy Guidance (ICPG) 801.1 to ensure that a set of validated and approved requirements is implemented using a disciplined process through development, integration, and testing within an established schedule and budget.
ICPG 801.1, Acquisition, 12 July 2007, Unclassified	Summary: As directed in Intelligence Community Directive (ICD) 801, the IC acquisition approach will follow the Intelligence Community Acquisition Model (ICAM) and will be either a single-step development or, more frequently, an evolutionary development. Both single-step and evolutionary developments are characterized by discrete phases (e.g., concept refinement, development, production, deployment, and sustainment) that correspond to the maturity of a technical solution to meet validated user requirements.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National



CGS Development Capability



Version 1.1.1

<p>National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified</p>	<p>Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.</p>
<p>Department of Defense (DoD)</p>	
<p>DoDD 5000.01, The Defense Acquisition System, 20 November 2007, Unclassified</p>	<p>Summary: Consistent with statute and the regulatory requirements specified in this directive and in Department of Defense Instruction (DoDI) 5000.02, every Program Manager (PM) shall establish program goals for the minimum number of cost, schedule, and performance parameters that describe the program over its entire lifecycle. PMs shall consider supportability, lifecycle costs, performance, and schedule comparable in making program decisions. Planning for operation and support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system lifecycle.</p>
<p>DoDI 5000.02, Operation of the Defense Acquisition System, 8 December 2008, Unclassified</p>	<p>Summary: This instruction implements Department of Defense Directive (DoDD) 5000.01 by establishing a simplified and flexible management framework for translating capability needs and technology opportunities based on approved capability needs, into stable, affordable, and well-managed acquisition programs that include weapon systems, services, and automated information systems. It describes the five phases of the Defense Acquisition Management System: Materiel Solution Analysis, Technology Development, Engineering & Manufacturing Development, Production & Deployment, and Operations & Support. Systems engineering shall be embedded in program planning and be designed to support the entire acquisition lifecycle.</p>
<p>DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007, Unclassified</p>	<p>Summary: This instruction establishes the DoD Information Assurance Certification and Accreditation Process (DIACAP) for authorizing the operation of DoD information systems. The process manages the implementation of information assurance (IA) capabilities and services and provides visibility of accreditation decisions. The DIACAP requirements, activities, and tasks described are applicable</p>



CGS Development Capability



Version 1.1.1

	throughout the information system's lifecycle, which includes development.
DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2007, Unclassified	Summary: IA shall be implemented in all system and services acquisitions at levels appropriate to the system characteristics and requirements throughout the entire lifecycle of the acquisition in accordance with (IAW) an adequate and appropriate Acquisition IA Strategy that shall be reviewed prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards.
CJCSM 3170.01C, Operation of the Joint Capabilities Integration and Development System (JCIDS), 1 May 2007, Unclassified	Summary: This manual sets forth guidelines and procedures for operation of the Joint Capabilities Integration and Development System (JCIDS) IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G, including the conduct of JCIDS analyses, the development of key performance parameters, and the JCIDS staffing process.
CJCSI 3170.01G, Joint Capabilities Integration and Development System (JCIDS), 1 March 2009, Unclassified	Summary: This instruction establishes the policies for the JCIDS. JCIDS procedures support the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council (JROC) in identifying and assessing joint military capability needs. This instruction focuses on the requirements process as implemented in JCIDS.
CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems, 15 December 2008, Unclassified	Summary: This instruction provides Joint Staff policy to ensure that Department of Defense (DoD) components develop, acquire, deploy, and maintain information technology (IT) and National Security Systems (NSS) that (1) meet the essential operational needs of U.S. forces; (2) are interoperable with existing and proposed Information Technology (IT) and National Security System (NSS) through standards, defined interfaces, modular design, and reuse of existing IT and NSS solutions; ... DoD combatant commands/services/agencies (C/S/A) play a key role in assuring consistent interoperability is appropriately inculcated into the capability's life cycle.
Defense Acquisition Guidebook, https://dag.dau.mil/Pages/Default.aspx , 17 December 2009,	Summary: This guidebook complements DoDD 5000.01 and DoDI 5000.02 by providing the acquisition workforce with discretionary best practice that should be tailored to the needs of each program. Section 4.3, Systems Engineering in the System Life Cycle, provides an integrated technical



CGS Development Capability



Version 1.1.1

Unclassified	framework for systems engineering activities throughout the acquisition phases of a system's lifecycle, highlighting the particular systems engineering inputs, activities, products, technical reviews, and outputs of each acquisition phase.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Development Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP-800-64 Rev 2, Security Considerations in the System Development	Summary: This special publication focuses on the information security components of the system development lifecycle (SDLC). It describes the key security roles and



CGS Development Capability



Version 1.1.1

<p>Life Cycle, October 2008, Unclassified</p>	<p>responsibilities that are needed in development of most information systems. Its scope is security activities that occur within the linear, sequential (a.k.a. waterfall) SDLC methodology. The five-step SDLC cited in this document [includes development] is an example of one method of development and is not intended to mandate this methodology.</p>
<p>Executive Branch (EO, PD, NSD, HSPD, ...)</p>	
<p>Nothing found</p>	
<p>Legislative</p>	
<p>Nothing found</p>	
<p>Other Standards Bodies (ISO, ANSI, IEEE, ...)</p>	
<p>IEEE 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process, 9 September 2005, Unclassified</p>	<p>Summary: This standard defines the interdisciplinary tasks that are required throughout a system's lifecycle to transform stakeholder needs, requirements, and constraints into a system solution. It is intended to guide the development of systems for commercial, government, military, and space applications and applies to projects within an Enterprise that is responsible for developing a product design and establishing the lifecycle infrastructure needed for lifecycle sustainment.</p>
<p>IEEE 1362-1998, IEEE Guide for Information Technology System Definition – Concept of Operations (CONOPS) Document, 19 March 1998, Unclassified</p>	<p>Summary: This guide provides approaches for developing a system that includes hardware, software, and people, manual procedures that cover major factors, such as schedule, cost, and risk that may affect a system. This is necessary for development for a dynamic environment.</p>
<p>ISO/IEC 15288:2008, Systems and Software Engineering-System Lifecycle Processes, 1 February 2008, Unclassified</p>	<p>Summary: This document provides a common process framework and the processes for acquiring and supplying systems. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the full system lifecycle (e.g., conception of ideas, development, production, utilization, support, and retirement of the system) and to the</p>



CGS Development Capability



Version 1.1.1

	acquisition and supply of systems.
ISO/IEC 19501:2005 Information Technology- Open Distributed Processing-Unified Modeling Language (UML) Version 1.4.2, Unclassified	Summary: This publication provides information on the topic “Software Development Methods,” which includes other methodologies for a comprehensive guidance of developing a design for a system.
International Council on Systems Engineering (INCOSE) Systems Engineering Handbook, version 3.1, 2007, Unclassified	Summary: This handbook describes the key process activities performed by systems engineers, covering in detail the purpose for each process activity, what needs to be done, and how to do it. It provides sufficient information to determine whether a given process activity is appropriate in supporting program objectives and how to go about implementing the process activity.
CMMI-DEV,v1.2, CMU/SEI 1-2006-008, ESC-TR-2006-008, August 2006, Unclassified	Summary: The technical solution in Capability Maturity Model Integration (CMMI) for Development (CMMI-DEV) includes additional information about designing, developing, and implementing solutions, including the design approaches, design concepts, and alternative solutions, which include those associated with measurement and the conduct of technical reviews.

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements



CGS Development Capability

Version 1.1.1



In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Scope of work-The complexity of systems being developed will be a factor contributing to their overall cost.
2. Storage requirements-There must be a secure code repository developers can use to store and access code. Version control may be an important feature.
3. Time to implement, maintain, and execute-Development is often a very lengthy process.
4. Manpower to implement, maintain, and execute-Many man-hours are required for completion, with multiple different skill sets.
5. Solution used for implementation-Developers will need access to specialized tools and testing environments.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Development Capability.

- The development phase of the lifecycle comprises many activities that ensure that IA is included from concept through deployment. The Enterprise shall include the incorporation of IA during architecture, concept, design, implementation/build, integration, requirements, and test.
- The Enterprise shall employ services from a program management role or office to ensure that all activities and resources are managed according to the program management plan and are able to meet the IA objectives established.
- The Enterprise shall provide visibility into the development activity to other programs with dependencies on the development activity.
- The Enterprise shall include the use of development processes that are established and approved in the Enterprise's policy and standards.
- The Enterprise shall define a CONOPS before developing requirements definitions. This CONOPS shall align with current standards and be documented and approved by the stakeholders.
- The Enterprise shall define security requirements that can be traced back to the solution architecture.
- All requirements shall be SMART.



CGS Development Capability



Version 1.1.1

- Requirements shall incorporate C&A requirements, interface interoperability requirements, and performance requirements.
- The requirements management process shall update and maintain the defined security requirements.
- All requirements shall be traceable to the architecture and shall be documented and maintained.
- Documentation (e.g., the requirements traceability matrix) shall align the requirements with the components and interfaces as part of the requirements decomposition, in accordance with the logical and physical architectures.
- All required levels of assurance (confidence that the security is effectively implemented) shall be established before verifications and validations are performed.
- Penetration testing, security testing, code review, and architecture review objectives shall be defined in accordance with the required assurance.
- All validations shall occur throughout the development, including the various stages of product integration.
- All security code reviews shall be automated and along with architecture reviews shall be conducted against incremental builds.
- All security code and architecture reviews shall be performed using accepted industry standards, such as UML.
- The Enterprise shall conduct functional and security testing in a mock operational environment that is consistent with the Enterprise's operational environment.
- Applications and products shall be tested on platforms different from the platforms on which they were developed.
- Penetration testing shall be performed against the solution during development.
- Testing shall be as automated as possible.
- Testing shall be performed by independent testers who shall be provided by the system security engineers (SSEs).
- All test plans and results shall be documented and stored in a central repository for future use.
- The test objectives shall trace to the requirements, which trace to the solution components.
- All test results shall be shared with the development team and stakeholders.
- SSEs shall ensure that the development team provides a solution that considers usability and maintainability of the security during the operations and maintenance phase of the lifecycle.



CGS Development Capability

Version 1.1.1



- The C&A and security requirements shall be understood, vetted, and accepted by the developers, independent testers, accrediting authority, and security stakeholders.
- All development activities (e.g., architecture, concept, design, implementation/build, integration, requirements, and test) shall be documented in accordance with industry standards and procedures.
- Peer and stakeholder milestone reviews shall be incorporated at each development activity stage. These periodic milestone reviews (as defined by the development schedule) shall include all stakeholders and shall have requirements acceptance prior to moving into the next stage of development.
- Milestone reviews shall include system requirements review and preliminary and critical design reviews.
- The development phase shall cover the configuration management of documentation.
- All documentation shall include product information along with required C&A documentation.
- Documentation shall follow versioning and control as defined by configuration management practices.