



National Security Agency/Central Support Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Portfolio Management Capability

Version 1.1.1

Portfolio Management is the process of analyzing, selecting, controlling, and evaluating Capability needs against current and planned investments within a Capability portfolio to better inform decision-makers and optimize resources. Portfolio Management involves the alignment of programs, initiatives, and activities with Enterprise priorities and requirements to maximize the return on investment. This Capability is specifically concerned with information assurance (IA) Portfolio Management, which is focused on the alignment of IA programs, initiatives, and activities.

07/30/2012



# CGS Portfolio Management 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 .....	6
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 .....	11
10	Cost Considerations .....	15
11	Guidance Statements.....	16



# CGS Portfolio Management 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 Portfolio Management 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.

Portfolio Management is the process of analyzing, selecting, controlling, and evaluating Capability needs against current and planned investments within a Capability portfolio to better inform decision-makers and optimize resources. Portfolio Management involves the alignment of programs, initiatives, and activities with Enterprise priorities and requirements to maximize the return on investment. This Capability is specifically concerned with information assurance (IA) Portfolio Management, which is focused on the alignment of IA programs, initiatives, and activities. This information will feed into the Enterprise's overall Portfolio Management Capability efforts.

## 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 Portfolio Management Capability provides the Enterprise with the ability to meet its IA capability needs. It provides decision-makers with the capability to manage their investments based on the defined needs. The Portfolio Management Capability relies on the Finance Capability to provide the business budget that measures IA resources' return on investment.

The Portfolio Management Capability shall be a resource-based Capability covering people, technology, and funding. The Capability activities shall be performed by a centralized, dedicated office that has visibility across the Enterprise, understands the IA needs, and can ensure cross-communication with the Portfolio Management Office. When resources are used across multiple activities, the Portfolio Management Office will have an understanding of the overall mission and the investments being made in the Enterprise to determine where duplication of effort may be occurring. IA Portfolio Management shall consider the IA technology lifecycle needs including technology refresh, such as the replacement of old technology and the Enterprise's risk posture changes. The Portfolio



# CGS Portfolio Management Capability



Version 1.1.1

Management Capability comprises four high-level activities: analyze, select, control, and evaluate.

## Analyze

The Portfolio Management Capability shall define the baseline, requirements, and gaps for the performance goals. The Portfolio Management Capability shall analyze IA goals and IA capabilities based on Enterprise needs. This analysis will determine the programs and initiatives (current and planned) that shall become or remain funded and will determine activity gaps. The Capability shall also determine a program's alignment with the Community Gold Standard (CGS) Framework.

Authoritative sources, such as U.S. Congress or other official bodies, shall be used when identifying the baseline dollars allocated to IA activities or programs. This use of authoritative sources shall help to prevent duplicate sources requesting resources for similar activities or initiatives. In some cases, requirements may need to be deconflicted to eliminate duplicate efforts and ensure alignment with Enterprise needs.

## Select

Based on analysis, the Portfolio Management Capability shall determine and select the best mix of investments. It shall use the priority, action, programmatic schedule, cost, and resources and compare them to a rating schema that is defined in this Capability by the Enterprise to determine which programs provide a robust combination of IA investments for the Enterprise. The rating schema shall be associated with the Enterprise's IA performance goals (such as detect, defend, respond). These prioritized current activities and other identified activities shall fill capability gaps in the Enterprise. Other agencies and Organizations may need to be consulted to determine what program best addresses a capability gap. Selection shall also include an analysis of programmatic trade-offs, such as cost, impact to risk posture, schedule, and resources. All selection criteria, security risk in particular, shall be weighted, by the Portfolio Management Office, to represent its alignment with CGS objectives and overall impact to security. The selection criteria shall be used to establish the overall benefit, feasibility, and cost of each selected IA investment. Subject matter experts from the Portfolio Management Office shall be used to assist in determining the appropriate weighting scheme for security risk.

## Control

As mentioned above, the Portfolio Management Capability shall determine the selected resources needed to implement the IA investments that will be used to fulfill the identified Enterprise IA capability gaps for the programs and projects. Acquisition of all needed



# CGS Portfolio Management Capability



Version 1.1.1

resources shall be obtained according to the Acquisition Capability. After selection and acquisition, the Portfolio Management Capability is responsible for oversight of the IA investments. To meet this responsibility, the Capability shall monitor and establish metrics to measure how programs are executing against their allotted funds. The Portfolio Management 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 established IA objectives. Overall, functional responsibilities for control are shared between the program manager role, program executive officers, and decision authorities. Programs shall be able to show their progress against the Enterprise performance goals selected. If the programs are not meeting the goals and schedules as defined, program decisions shall realign funds and resources, as applicable, to another program to facilitate meeting the Enterprise's IA goals or remove funds from a program until the initial program aligns with defined goals and schedule.

Control reporting mechanisms shall consist of program status reviews held with the budget decision authority, the IA authority, and technical oversight officials. These reviews shall include current activities and achievements as they relate to the project's intended IA performance goals. Reporting shall be performed as frequently as the Portfolio Management Office deems necessary in accordance with budget decision needs. Additional reporting mechanisms shall be in place to address, in a timely manner, technical and budget issues and concerns as they arise.

## Evaluate

In addition to monitoring and oversight information, the Portfolio Management Capability shall evaluate the metrics that are measured against the performance goals. Data gathering for the IA initiatives shall relate to the Capability or program being measured. Once the metrics information is gathered, the Enterprise shall assess how effective the Capabilities are at meeting the goals based on the metrics and investment portfolio. Evaluation activities provide input back into analysis activities for portfolio management, and a cyclic process continues in order to make necessary adjustments. In the event of a mitigating circumstance, such as a change in the Enterprise's performance goals, the Portfolio Management Capability may need to perform a portion of the process without first completing the full cycle of activities. This shall also determine the frequency of evaluations and the remaining Portfolio Management activities.

The Portfolio Management Capability shall ensure that all IA portfolio data is stored and accessible for all programs. The information contained in the portfolio shall include program, project, activity name, responsible Organization, schedule, budget, performance



# CGS Portfolio Management Capability



Version 1.1.1

goal alignment, and dependencies (on other programs, projects, and activities), and current and future activities. This information shall be protected in accordance with the Data Protection, System Protection, and Access Management Capabilities. Information shall be linked such that information is not duplicated in the portfolio. Highly sensitive data shall be referenced where the data cannot be provided in the portfolio itself. In addition, the Capability's format shall facilitate sharing of information.

## 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 established an overall Portfolio Management Office.
2. The budget is known.
3. The Organization understands the CGS Framework and its intended use.
4. New requirements are provided.
5. Information from other Organization's IA activities is available.
6. The Organization knows its resources before any decisions are made.
7. 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 aligns resources as needed to support missions.
2. The Capability periodically assesses its resources and their alignment to ensure alignment with performance goals.
3. The Capability defines priorities based on the IA performance goals, risk, security posture, subject matter expert input, and trade-offs.

## 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



# CGS Portfolio Management Capability



Version 1.1.1

Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When Portfolio Management is performed correctly, the Organization will possess a capability to define IA performance goals, gaps, and metrics. The IA performance goals will be based on the Organization-specific goals, such as prevent, detect, respond, and integrate, which will help the Organization to determine how the CGS is used in its Enterprise.

The Organization will use authoritative sources to define its IA requirements. The Organization will establish IA performance goals using the outlined steps in the Gold Standard Guidance section. Based on the goals and requirements, the Organization will assess the gaps.

As part of the Portfolio Management Capability, the Organization will define and use a rating schema to measure IA performance goals for CGS Capabilities. The Organization will use Portfolio Management to analyze Capabilities against each other. Thus, the Organization will be managing the portfolio for all the Capabilities.

The Organization will determine the baseline for a Capability based on the allotted IA funds issued from the Organization's authoritative source. The Organization's Portfolio Management Office will conduct an analysis of the IA capability needs to determine the needs based on current and future investments. This information will also be used to determine the Organization's Capability gaps. The Organization will decide on the IA investments needed for a Capability. In addition, an Organization will determine the IA performance goals that are being prevented based on the goals that are not being met and determine desired goals that can be accomplished.

The Organization will determine the best combination of investments for a Capability through type of priority, action, programmatic schedule, cost, and resources. The Organization will then select the best mix of investments for the portfolio. This will be based on the rating schema (which is determined by the Portfolio Management Office) that is measured against the IA performance goals to detect any unnecessary spending. The Organization will realign funds between IA investments to optimize execution in accordance with performance goals.

The Organization will oversee the execution of the funding for a Capability. The Organization will ensure that the execution of funding against the IA performance goals is



# CGS Portfolio Management Capability



Version 1.1.1

on target through technical reviews and status reporting to communicate the intended goal to the budget decision authority and other stakeholders (e.g., controllers).

The Organization will evaluate the IA Portfolio on an ongoing basis. To execute evaluation, the Organization will use the metrics and IA performance goals being measured for a Capability. This will be accomplished through gathering information and evaluating expected outcome of the investments for a Capability. The Organization will then integrate, into a Capability, information for the IA performance goals that are being measured.

An Organization will use resources (e. g., people and technology) across the Enterprise to gain an understanding of the scope of IA activities and initiatives for the Portfolio Management Capability. To ensure that there are no duplicate efforts, an Organization will have oversight through the Portfolio Management Office for a broad understanding (e.g., IA lifecycle product needs, technology refresh, and risk posture) of investments needed for a mission.

An Organization will manage and store the portfolio, centrally. In addition, an Organization will ensure that the portfolio is accessible for current and future efforts of the Organization. An Organization will rely on other CGS Capabilities to ensure the protection of the Portfolio Management Capability information (See Data Protection, System Protection and Access Management CGS Capabilities).

## 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 Portfolio Management Capability relies on the Network Mapping Capability for information used to understand the status of Enterprise assets and operations.



# CGS Portfolio Management Capability



Version 1.1.1

- Network Boundary and Interfaces—The Portfolio Management Capability relies on the Network Boundary and Interfaces Capability for information used to understand the status of Enterprise assets and operations.
- Utilization and Performance Management—The Portfolio Management Capability relies on the Utilization and Performance Management Capability for information that highlights deficiencies (or less than optimal circumstances) in operations.
- Understand Mission Flows—The Portfolio Management Capability relies on the Understand Mission Flows Capability for information that provides mission context and meaning for people, process, technology, and environment, which contributes to investment decisions.
- Understand Data Flows—The Portfolio Management Capability relies on the Understand Data Flows Capability for information used to understand the status of Enterprise assets and operations.
- Hardware Device Inventory—The Portfolio Management Capability relies on the Hardware Device Inventory Capability for information used to understand the status of Enterprise assets and operations.
- Software Inventory—The Portfolio Management Capability relies on the Software Inventory Capability for information used to understand the status of Enterprise assets and operations.
- Understand the Physical Environment—The Portfolio Management Capability relies on the Understand the Physical Environment Capability for information used to understand the status of Enterprise assets and operations.
- Risk Analysis—The Portfolio Management Capability relies on the Risk Analysis Capability to provide information regarding the Enterprise the risk posture.
- Risk Monitoring—The Portfolio Management Capability relies on the Risk Monitoring Capability to provide information regarding the Enterprise security posture, which contributes to investment decisions.
- Finance—The Portfolio Management Capability relies on the Finance Capability to ensure that the resources are budgeted and provided for IA activities and initiatives.
- Acquisition—The Portfolio Management Capability relies on the Acquisition Capability to procure IA resources that support and comply with the mission.

## 7.2 Core Interrelationships

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

- IA Policies, Procedures, and Standards—The Portfolio Management Capability relies on the IA Policies, Procedures, and Standards Capability to provide



# CGS Portfolio Management Capability



Version 1.1.1

information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness–The Portfolio Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Portfolio Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Portfolio Management 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.

- Development–The Portfolio Management Capability relies on the Development Capability to provide information about the status of resources against performance goals.
- Deployment–The Portfolio Management Capability relies on the Deployment Capability to provide information about the status of resources against performance goals.
- Operations and Maintenance–The Portfolio Management Capability relies on the Operations and Maintenance Capability to provide information about the status of resources against performance goals.
- Decommission–The Portfolio Management Capability relies on the Decommission Capability to provide information about the status of resources against performance goals.

## 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>



# CGS Portfolio Management Capability



Version 1.1.1

<p>PM-3 <i>INFORMATION SECURITY RESOURCES</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> <li>a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;</li> <li>c. Ensures that information security resources are available for expenditure as planned.</li> </ul> <p>Enhancement/s: None Specified.</p>
<p>PM-11 <i>MISSION/BUSINESS PROCESS DEFINITION</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> <li>a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and</li> <li>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.</li> </ul> <p>Enhancement/s: None Specified</p>
<p>SA-2 <i>ALLOCATION OF RESOURCES</i></p>	<p>Control: The organization:</p> <ul style="list-style-type: none"> <li>a. Includes a determination of information security requirements for the information system in mission/business process planning;</li> <li>b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and</li> </ul> <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.

### Portfolio Management Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 500 Director of National Intelligence, Chief Information Officer, August	Summary: This directive establishes the responsibilities of the Associate Director of National Intelligence/Chief Information Officer (ADNI/CIO). The CIO is to develop an



# CGS Portfolio Management Capability



Version 1.1.1

2008, Unclassified	Enterprise architecture for the Intelligence Community (IC) and ensure all IC components comply with the IC architecture and to direct and manage all information technology (IT) related procurements to ensure they achieve the IC's strategic goals. In addition, the IC CIO is to monitor the performance of IT programs of the IC and advise the DNI regarding whether to continue, modify, or terminate a program or project. This describes a Portfolio Management function.
Draft IC CIO Council Charter, 11 November 2009	Summary: The IC CIO Council serves as the IC's senior information and enabling technology governance body supporting the IC CIO and the IC. The charter addresses investments and Portfolio Management.
<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
<b>Department of Defense (DoD)</b>	
DoDD 5100.20, National Security Agency/Central Security Service (NSA/CSS) 26 January 2010, Unclassified	Summary: This directive established policy to update the mission, organization, and management; responsibilities and functions; relationships; authorities; and administration pertaining to portfolio management. This directive shall be interpreted consistent with law, policy, and IA; manage the GIG IA portfolio, consistent with the processes and procedures; and make IA portfolio investment recommendations to the ASD(NII)/DoD CIO to ensure the efficient and effective delivery of capabilities to the warfighter and to maximize return on investment to the Enterprise.
DoDD 5144.1 Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer	Summary: This directive establishes responsibilities for the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)): The ASD(NII)/DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and



# CGS Portfolio Management Capability



Version 1.1.1

<p>(ASD(NII)/DoD CIO), 2 May 2005, Unclassified</p>	<p>network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; IT, including National Security Systems (NSS); information resources management (IRM) (as defined by reference (b)); spectrum management; network operations; information systems; IA; positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters. Pursuant to chapter 113, subchapter III of 40 U.S.C. (reference (j)), the ASD(NII)/DoD CIO has responsibilities for integrating information and related activities and services across the department. The ASD(NII)/DoD CIO also serves as the DoD Enterprise-level strategist and business advisor from the information, IT, and IRM perspective; Information and IT Architect for the DoD enterprise; and, DoD-wide IT and IRM Executive. Hereafter these responsibilities and functions are referred to collectively as “NII and CIO” (including IRM) matters.</p>
<p>DoDD 7045.20 Capability Portfolio Management, 25 September 2008, Unclassified</p>	<p>Summary: This document establishes policy and assigns responsibilities for the use of capability portfolio management in order to advise senior leadership on capability investment pursuant to the authority vested in the Secretary of Defense by section 113 of title 10, United States Code.</p>
<p>DoDD 8000.01, Management of DoD Information Enterprise, 10 February 2009, Unclassified</p>	<p>Summary: This directive establishes policy that all aspects of the Department of Defense (DoD) information Enterprise, including the Global Information Grid (GIG) infrastructure and Enterprise services and solutions, shall be planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a DoD net-centric environment. The DoD Enterprise Architecture shall be maintained and applied to guide investment portfolio strategies and decisions to establish and enforce standards and guide security and information assurance (IA) requirements across the DoD. It also sets policy, which requires the review of all IT investments for compliance with</p>



# CGS Portfolio Management Capability



Version 1.1.1

	these architectures and IT standards.
DoDD 8115.01, Information Technology Portfolio Management, 10 October 2005, Unclassified	Summary: This directive establishes policy requiring all IT investments shall be managed as portfolios to ensure IT investments support the department's vision, mission, and goals; ensure efficient and effective delivery of capabilities to the warfighter; and maximize return on investment to the Enterprise. Each portfolio shall be managed using the GIG architecture.
DoDI 8115.02 Information Technology Portfolio Management Implementation, 30 October 2006, Unclassified	Summary: This instruction (b) Describes responsibilities for the management of DoD information technology (IT) investments as portfolios within the DoD Enterprise (to include Mission Areas, Subportfolios, and Components) that focus on improving DoD capabilities and mission outcomes.
DoDI 8410.02 NetOps for the Global Information Grid (GIG), 19 December 2008, Unclassified	Summary: This instruction established ASD(NII) responsibilities: e. Develop NetOps capability increments in collaboration with functional owners and Capability Portfolio Managers to ensure efficient and secure GIG operations.
DoDD 8500.01E Information Assurance, 23 April 2007, Unclassified	Summary: This directive established policy: 4.3. Information Assurance shall be a visible element of all investment portfolios incorporating DoD-owned or -controlled information systems, to include outsourced business processes supported by private sector information systems and outsourced information technologies; and shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives...
<b>Committee for National Security Systems (CNSS)</b>	
Nothing found	
<b>Other Federal (OMB, NIST, ...)</b>	
Nothing found	
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
Nothing found	
<b>Legislative</b>	



# CGS Portfolio Management Capability



Version 1.1.1

Nothing found	

## Portfolio Management 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, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	

## 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



# CGS Portfolio Management Capability



Version 1.1.1

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

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

1. Solution used for implementation—This Capability will require specialized tools to carry out its functions.
2. Storage requirements—Information about currently held resources and assets will need to be stored such that it is accessible when needed. Communications to and from the storage medium need to be protected.

## 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 Portfolio Management Capability.

- The Enterprise shall provide its decision-makers with the ability to manage their investments based on their IA capability needs.
- Portfolio management shall be a resource-based system that addresses people, technology, and funding.
- Portfolio management activities shall be performed by a centralized, dedicated office that has visibility across the Enterprise, understands the IA needs, and can ensure cross-communication with a portfolio management office.
- A portfolio management office shall have an understanding of the overall mission and the investments being made in the Enterprise to determine where duplication of effort may be occurring.
- IA portfolio management shall consider the IA technology lifecycle needs, including technology refresh and replacement of old technology.
- The portfolio management system shall define the baseline, requirements, and gaps for the performance goals.



# CGS Portfolio Management Capability



Version 1.1.1

- The portfolio management system shall analyze IA goals and IA capabilities based on Enterprise needs to determine gaps.
- The portfolio management system shall determine a program's alignment with the CGS Framework.
- The portfolio management system shall use official bodies, including US Congress, when identifying the baseline dollars allocated to IA activities or programs to prevent duplicate sources from requesting resources for similar activities or initiatives.
- The portfolio management system shall determine and select the best mix of investments using priority, action, programmatic schedule, cost, and resources and compare them to determine which programs provide a robust combination of IA investments for the Enterprise.
- The rating schema used to determine and select the best mix of investments shall be associated with the Enterprise's IA performance goals (such as detect, defend, respond).
- The selection of the best mix of investments shall also include an analysis of programmatic trade-offs, such as cost, impact to risk posture, schedule, and resources.
- All selection criteria, security risk in particular, shall be weighted by the portfolio management office to represent its alignment with Enterprise IA objectives and overall impact on security.
- The selection criteria shall be used to establish the overall benefit, feasibility, and cost of each selected IA investment.
- The portfolio management system shall determine the selected resources needed to implement the IA investments that will be used to fulfill the identified Enterprise IA capability gaps for the programs and projects.
- Subject matter experts from the portfolio management office shall be used to assist in determining the appropriate weighting scheme for security risk.
- The portfolio management system shall be responsible for oversight of the IA investments for the Enterprise.
- The portfolio management system shall monitor established metrics to measure how programs are executing against their allotted funds.
- The portfolio management system 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 established IA objectives.



# CGS Portfolio Management Capability



Version 1.1.1

- Programs shall be able to show their progress against the selected Enterprise performance goals.
- If the programs are not meeting the goals and schedules as defined, program decisions shall realign funds and resources, as applicable, to another program to facilitate meeting the Enterprise's IA goals or remove funds from a program until the initial program aligns with defined goals and schedule.
- Control reporting mechanisms shall consist of program status reviews held with the budget decision authority, the IA authority, and technical oversight officials and shall include current activities and achievements as they relate to the project's intended IA performance goals.
- All reporting shall be performed in accordance with Enterprise budget needs and technical issues, as needed.
- The portfolio management system shall evaluate the metrics that are measured against the performance goals.
- Data gathering for the IA initiatives shall relate to the capability or program being measured to assess effectiveness of investments.
- In the event of a mitigating circumstance, such as a change in the Enterprise's performance goals, the portfolio management system may need to perform a portion of the process without first completing the full cycle of activities. This shall also determine the frequency of evaluations and the remaining portfolio management activities.
- The portfolio management system shall ensure that all IA portfolio data is stored and accessible for all programs.
- The information contained in the portfolio shall include program, project, activity name, responsible Organization, schedule, budget, performance goal alignment, and dependencies (on other programs, projects, and activities), and current and future activities.
- All detail information, including sensitive data, contained in the portfolio shall be protected in accordance with other systems on the Enterprise and shall be linked such that information is not duplicated in the portfolio.
- All formatting used by the portfolio management system shall facilitate sharing of information.