



# Command, Control, Communication, Computers and Information Technology (C4&IT)

## Strategic Plan



FY11-FY15



Intentionally Blank



## To the Men and Women of the Coast Guard:

I am pleased to present the U.S. Coast Guard's *Command, Control, Communication, Computers, and Information Technology (C4IT) Strategic Plan for Fiscal Years 2011-2015*. Since the initial publication of our C4IT Strategic Plan in FY08, we have made major strides in improving our C4IT capabilities throughout the Coast Guard. By continuing on this sound course, we will provide the Coast Guard with the C4IT capabilities it needs to save lives, safeguard our maritime borders, respond to natural and man-made disasters, interdict illegal drugs, and move commerce across the high seas.



This strategic plan is driven by Federal and Departmental guidance and the Commandant's guiding principles: steady the service, honor our profession, strengthen our partnerships, and respect our shipmates. The C4IT Strategic Plan identifies the scope and direction of Coast Guard C4IT development, investment and infrastructure for the next five years. By closing gaps in the five core areas listed below, the Coast Guard will have the C4IT capabilities it needs to support mission execution

- Information:** Improve and encourage information sharing, quality, efficiency, and compliance with internal and external partners.
- Technology:** Deliver mission-focused, interoperable, and innovative C4IT solutions for the enterprise.
- Security:** Enhance mission effectiveness by preventing C4IT security incidents, such as cyber attacks and intrusions, and enhancing C4IT security mitigation, awareness, and compliance.
- Governance:** Govern the C4IT enterprise through the execution of technical authority and effective processes for enterprise architecture, capital planning and investment control, systems development, project management, performance measurement and requirements.
- Organizational Excellence:** Achieve C4IT organizational excellence by continually developing our workforce, collaborating with internal and external partners, and improving business processes.

Each year we update the CG-6 Performance Plan (Appendix A) to reflect our ongoing commitment to this strategy. By aligning our world of work to the goals listed above, we guarantee that our limited resources are being used to effectively accomplish the Coast Guard's overarching strategy for C4IT.

The success of this strategic plan depends on the talents, commitment and proactive involvement of the entire Coast Guard community. We look forward to continuing to work with all of our stakeholders and operational partners to achieve our mutual goals of maritime safety, security and stewardship.



**Rear Admiral Robert E. Day Jr.**

*Assistant Commandant for Command, Control, Communications, Computers and Information Technology  
Chief Information Officer  
Director, Coast Guard Cyber Command, Pre-Commissioning Detachment  
United States Coast Guard*

## Table of Contents

INTRODUCTION.....	5
Purpose.....	5
Scope.....	5
Authority.....	5
BACKGROUND.....	6
Current Environment.....	6
Challenges.....	6
Strategic Guidance.....	7
CG-6 MISSION & VISION.....	12
Mission.....	12
Vision.....	12
Core Values and Concepts.....	12
CG-6 GOALS AND OBJECTIVES.....	13
Overview.....	13
Goal 1: Information.....	14
Goal 2: Technology.....	15
Goal 3: Security.....	16
Goal 4: Governance.....	17
Goal 5: Organizational Excellence.....	18
THE WAY AHEAD.....	19
APPENDIX A: CG-6 PERFORMANCE PLAN.....	21
APPENDIX B: STRATEGIC ALIGNMENT MATRICES.....	85
APPENDIX C: ACRONYMS.....	92
APPENDIX D: DEFINITIONS.....	97
APPENDIX E: REFERENCES.....	99
APPENDIX F: DOCUMENT CHANGES.....	100



# INTRODUCTION

## PURPOSE

The Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C4IT)/CG-6, Chief Information Officer (CIO), for the Coast Guard publishes this C4IT Strategic Plan. The purpose of this plan is to provide a unifying strategy for CG-6 to improve, integrate, and maximize the Coast Guard's C4IT capabilities in support of mission execution.

## SCOPE

The intent is for members of the C4IT community and Coast Guard to use this plan to establish and prioritize recommendations for implementing improvements to the Coast Guard's C4IT infrastructure, systems, applications, products, policies, practices, and processes. The focus of this document is on activities that must occur in the next five years to begin achieving the long term goals of the Coast Guard and the Department of Homeland Security (DHS). While the goals in this plan may not be fully realized in the next five years, it is clear that coordinated activity must occur now to improve the Coast Guard's operational capabilities.

## AUTHORITY

The C4IT Strategic Plan has been developed under the authority of the Assistant Commandant for C4IT, CIO, for the Coast Guard. CG-6 derives its authority for C4IT from Commandant Instruction (COMDTINST) 5401.5, Establishment of the CG-6 Directorate and Associated Duties. This COMDTINST made CG-6 the office responsible for all Coast Guard operational, business, and infrastructure C4IT assets.

At a departmental level, DHS Management Directive (MD) 0007.1, Information Technology Integration and Management, establishes the component CIO as the authority responsible for the timely delivery of Information Technology (IT) mission services. This includes the effective management and administration of all component IT resources to meet mission, departmental, and enterprise program goals.

At a Federal level, U.S. Code Title 44, Public Printing and Documents, Federal Information Policy mandates three key responsibilities for the CIO. One, the CIO must develop and maintain a strategic information resources management plan. Two, the CIO must establish goals for improving information resources' contribution to program productivity, efficiency, and effectiveness. Three, the CIO must identify methods for measuring progress towards reaching those goals. This plan addresses each of these federally mandated responsibilities.



# BACKGROUND

## CURRENT ENVIRONMENT

The U.S. Coast Guard, one of the nation's five armed services, is the principal Federal agency responsible for maritime safety, security, and stewardship. As such, we protect the vital economic, environmental, and security interests of the United States. This includes the personal safety and security of the maritime public, our natural and economic resources, the global commerce infrastructure, and the integrity of our maritime borders. We are committed to addressing all threats and hazards in a manner consistent with the law and in alignment with the goals and objectives of DHS. We do this throughout the maritime domain including in U.S. ports and inland waterways, along the coasts, on the high seas, and in other regions where our maritime equities are at stake.

As a military, multi-mission, and maritime service, we have three fundamental roles: maritime safety, security, and stewardship. In each of these roles, the Coast Guard depends on C4IT to achieve its missions.

From Miami to Juneau, in Coast Guard command centers across the United States, we use C4IT systems to capture information about suspicious activities and possible threats. On our 200 ships, 250 aircraft, and 1,700 boats, we deploy C4IT assets, such as radios and sensors, to keep our forces connected with internal and external partners on shore, along the coasts, and on the high seas. To support the missions of the Coast Guard, our 89,000 military, civilian, and auxiliary employees use over 42,000 computers, 20,000 radios, and 700 different types of C4IT products to perform their work each day.

## CHALLENGES

We operate in a continually changing and complex mission environment. As such, the way ahead poses many challenges for the Coast Guard. This is especially true in the area of C4IT as the Coast Guard becomes more dependent on technology for mission execution. As the Directorate for C4IT (CG-6), we must adapt our goals, objectives, and initiatives to fulfill the Coast Guard's complex and continually changing mission and business needs.

The following sections outline some of the challenges that we currently face as the Coast Guard's Directorate for C4IT.

- **Balance Between Missions:** After September 11, 2001, the Coast Guard's priorities and focus shifted suddenly and dramatically. Today and into the future, as a component of DHS, the Coast Guard must dedicate more resources to homeland security missions. In addition, any unexpected event, from a man-made disaster (such as a terrorist attack) to a natural disaster (such as a hurricane), may result in a shift in resources. Further complicating this balance between missions is Coast Guard's requirement, as a military service, to remain ready and prepared to respond to the needs of the Department of Defense (DoD). To fulfill these varied roles, we must ensure that our technology is agile and mission-focused.
- **Interoperability with Partners:** The Coast Guard must be able to effectively interoperate and share information across a wide range of inter- and intra-agency partners to support disaster relief, law



enforcement, defense, and other mission and business areas. This demand for information sharing and interoperability is not a new issue. Previous events, such as Hurricane Katrina, prove that information sharing and interoperability can lead to mission success. Consequently, we must implement compatible equipment and standards, and define procedures and practices for information sharing to ensure seamless communications with our partners.

- **Increasing Demands Against a Relatively Constant Budget:** User expectations and requirements continually increase as technology advances. At the same time, the overall funding available for C4IT investment remains relatively constant. As demands increase, we must improve our ability to prioritize investments to achieve maximum results with our scarce resources.
- **Increasing Threats to Network and Information:** From capturing intelligence about a possible threat to transmitting employee information, we rely on our network to exchange, process, and store information 24 hours a day, 7 days a week. We must protect and defend this vital resource to assure network and information confidentiality, integrity, availability, and privacy at all times.
- **Rapid Pace of Technology Advancement:** Technology is progressing at an ever increasing pace. This represents a significant challenge and opportunity for the Coast Guard. As we advance, we must balance the incorporation of new technologies that improve our operational capabilities with our limited resources and funding. We must be prepared to provide innovative services to our customers by re-thinking our current C4IT approaches as technology advances.
- **Rising Customer Expectations:** As new technology becomes available and commonplace in the market, Coast Guard personnel continue to find new ways to leverage C4IT to perform their jobs more effectively. As technology advances, we must make informed decisions about how to deploy new capabilities to fulfill rising customer expectations.

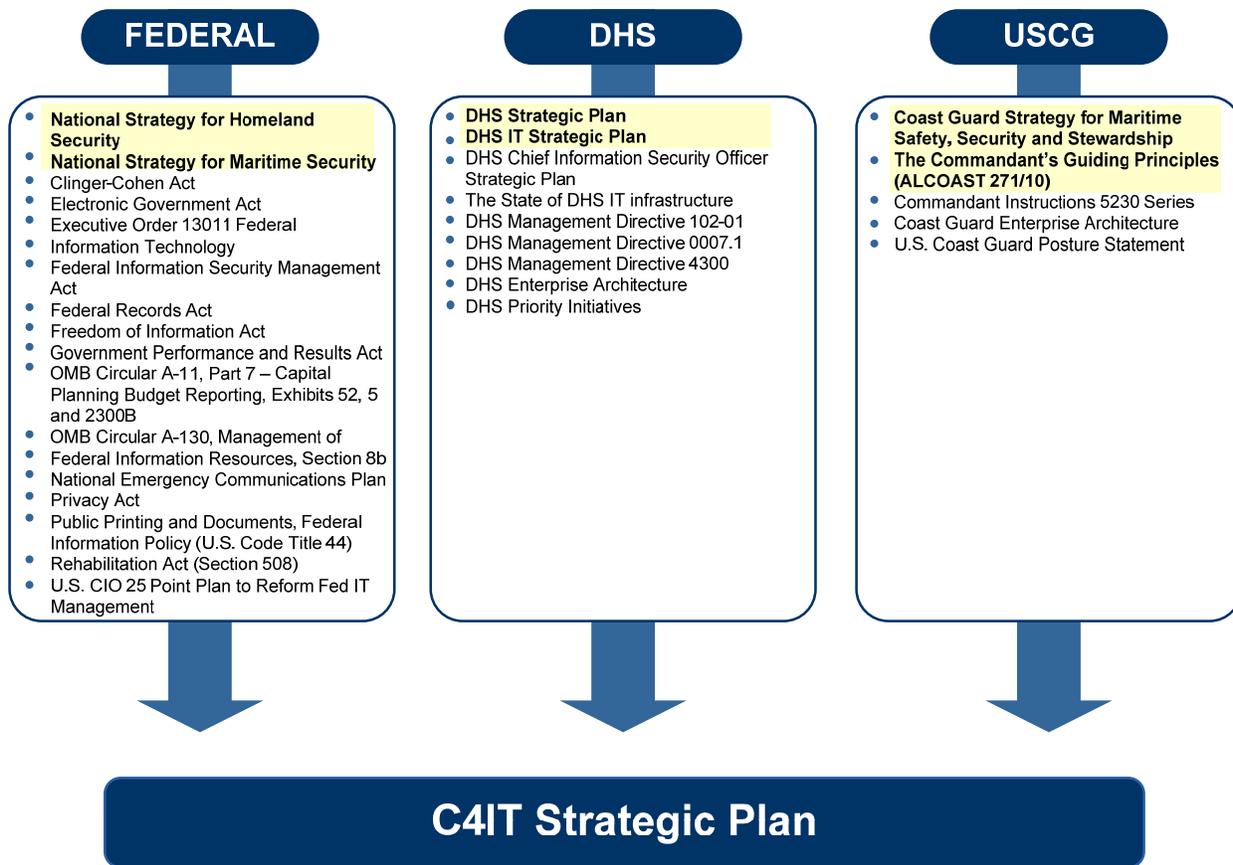
These are but a few of the challenges that the Coast Guard must address. Our ability to select the appropriate strategies to meet these challenges will enable Coast Guard success in the future. By implementing this C4IT Strategic Plan, and the related CG-6 Performance Plan (Appendix A), we will systematically and comprehensively resolve each of these challenges.

## STRATEGIC GUIDANCE

By understanding and aligning our goals to Federal, DHS, and Coast Guard strategic guidance, we can enhance Coast Guard mission execution.

Figure 1 shows how Federal, DHS, and Coast Guard guidance shaped the goals, objectives, and initiatives identified later in this plan. Highlighted at the top of each box in Figure 1 are the specific guidance documents that we discuss in more detail in the following sections.





 Described in the following sections

**Figure 1: C4IT Strategic Plan Guidance**

## Federal Guidance

The *National Strategy for Homeland Security* serves to guide, organize, and unify our Nation's homeland security efforts. It recognizes that we must continue to focus on a persistent and evolving terrorist threat while addressing the full range of potential catastrophic events that impact homeland security.

The following goals, from the *National Strategy for Homeland Security*, guide the Nation's homeland security activities:

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources;
- Respond to and recover from incidents that do occur; and
- Continue to strengthen the foundation to ensure our long-term success.

In addition, the *National Strategy for Maritime Security* (NSMS) serves to integrate and synchronize the existing DHS strategies for maritime security and ensure their effective and efficient implementation. The following objectives from the NSMS guide the Nation's maritime security activities:



- Prevent Terrorist Attacks and Criminal or Hostile Acts: Detect, deter, interdict, and defeat terrorist attacks, criminal acts, or hostile acts in the maritime domain, and prevent its unlawful exploitation for those purposes.
- Protect Maritime-Related Population Centers and Critical Infrastructures: Protect maritime-related population centers, critical infrastructure, key resources, transportation systems, borders, harbors, ports, and coastal approaches in the maritime domain.
- Minimize Damage and Expedite Recovery: Minimize damage and expedite recovery from attacks within the maritime domain.
- Safeguard the Ocean and Its Resources: Safeguard the ocean and its resources from unlawful exploitation and intentional critical damage.

## DHS Guidance

The United States Government established DHS to secure the American homeland and protect the American people. The *U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008-2013*, interprets the *National Strategy for Homeland Security* and prescribes the homeland security vision for the DHS workforce, DHS stakeholders, and the American people. The following goals from the *DHS Strategic Plan* guide the breadth of our activities at the Coast Guard.

- Goal 1: Protect our Nation from dangerous people.
- Goal 2: Protect our Nation from dangerous goods.
- Goal 3: Protect critical infrastructure.
- Goal 4: Strengthen our Nation's preparedness and emergency response capabilities.
- Goal 5: Strengthen and unify DHS operations and management.

Specifically for IT, the DHS CIO established four strategic goals for enhancing the Department's IT capabilities in support of the mission objectives in the *DHS Information Technology Strategic Plan 2011-2015*:

- Goal 1: Establish secure IT services and capabilities to protect the Homeland and enhance our Nation's preparedness, mitigation and recovery capabilities.
- Goal 2: Strengthen and unify the Department's ability to share information and services internally and with Federal, State, local, tribal, international and private industry partners.
- Goal 3: Improve transparency, accountability, and efficiencies of services and programs through effective governance.
- Goal 4: Develop and implement a comprehensive approach to IT employee recruitment, development, retention and recognition to ensure excellence in IT delivery across the Department.



The Coast Guard's C4IT goals directly align to the Department's IT goals (see Appendix B for matrices). The alignment of these two sets of goals helps to ensure that our C4IT goals and objectives fully support the Department's goals. The synchrony also provides opportunities to collaborate with the other components within DHS as they work to achieve the same goals.

## U.S. Coast Guard Guidance

### The Commandant's Guiding Principles

In ALCOAST 271/10 (dated May 20, 2010), Admiral Bob Papp published four guiding principles for his watch as Commandant. These principles challenge people, at every level of the chain of command, to refocus on their missions to ensure that our waterways are safe and secure. Admiral Papp's four guiding principles are as follows:

**Steady the service:** To reduce stress on our service and maintain the highest level of readiness we must emphasize our statutory missions, finish organizational realignment and prioritize demands for our services within the budget. We must continue to pursue replacement assets for the future. We must return to a sustainable state.

**Honor our profession:** At all times, we are a military organization guided by responsibility, authority and accountability. Mission excellence is our north star. Honoring our profession requires inspired leadership to develop knowledge, skills, pride and experience, in a nurturing environment, built from a foundation of clear doctrine and training.

**Strengthen our partnerships:** They are a force multiplier. As demand for our service continues to expand, and the threats in the maritime environment increase in complexity, a unilateral approach will not be the best or the most efficient means to achieve mission success. We can be more effective and provide greater value to our country when we forge partnerships with local, state, federal, tribal and international agencies. For the same reasons, strengthening appropriate relationships with private industry is imperative. Ultimately, strong partnerships are critical to enhancing our capability, effectiveness and credibility in the maritime domain.

**Respect our shipmates:** Our people are the Coast Guard's greatest asset and our ability to perform our mission ultimately depends on your health, vibrancy, training and capabilities. We must provide the best in human resource management, administrative support, wellness programs and professional development, while maintaining a safe, collaborative and productive work environment. Our service must also draw strength from the diversity of our nation.

-Admiral Bob Papp, Commandant, U.S. Coast Guard, ALCOAST 271/10



## Coast Guard Strategy for Maritime Safety, Security, and Stewardship

This strategy is the framework and strategic intent that guides our activities at the Coast Guard. More specifically, it identifies the following priorities for improving the Nation's preparedness and advancing U.S. maritime interests.

- **Strengthening Regimes for the U.S. Maritime Domain:** The Coast Guard will work with DHS, interagency partners, U.S. maritime stakeholders, and the international community to update and strengthen existing maritime regimes and put in place new regimes where needed to address emerging challenges and threats.
- **Achieving Awareness in the Maritime Domain:** The Coast Guard will work with the DoD, U.S. interagency partners, state and local governments, the private sector, and the international community to implement the *National Plan to Achieve Maritime Domain Awareness* as intended by the NSMS.
- **Enhancing Unity of Effort in Maritime Planning and Operations:** The Coast Guard will improve its integrated planning with all partners, its network of command and control centers, and its operational capabilities. In doing this, the Coast Guard will advance unity of command where possible, and unity of effort at all times. The Coast Guard will also align its operational structure around shore based, maritime patrol, and deployable specialized forces to better allow force packaging and scalable response to all threats and all hazards. This will support the NSMS and its *Maritime Operational Threat Response Plan (MOTR)*, as well as the *National Response Plan*.
- **Integrating Coast Guard Capabilities for National Defense:** The Coast Guard will better integrate its capabilities with DoD and optimize its forces within a Navy/Coast Guard relationship. This will build upon the "National Fleet" model and support the *National Maritime Strategy (NMS)* as well as the NSMS and its subordinate plans.
- **Developing a National Capacity for Maritime Transportation System Recovery:** To support the NSMS and its *Maritime Infrastructure Recovery Plan (MIRP)*, the Coast Guard will leverage its authorities, responsibilities, and capabilities to lead the national planning agenda for assuring the continuity of commerce and critical maritime activities.
- **Focusing International Engagement on Maritime Governance:** The Coast Guard will focus its international efforts to assist maritime organizations and partner nations in building the sustainable regimes, awareness, and operational capabilities necessary to improve the governance of the global maritime domain.



# CG-6 MISSION & VISION

## MISSION

The Assistant Commandant for C4IT/CG-6 designs, develops, deploys, and maintains the Coast Guard's C4IT solutions. These solutions enable mission execution and help the Coast Guard achieve its goals of maritime safety, security, and stewardship.

## VISION

A Coast Guard that is ready with the right information for the right people at the right time to safeguard the Nation's maritime domain.

## CORE VALUES AND CONCEPTS

Interrelated core values and concepts guide the way we, as CG-6, conduct business. These core values and concepts are summarized below.

- **C4IT Leadership:** We believe that C4IT leaders must set clear technology direction, have high expectations for system delivery, create a customer-focused culture, and balance the needs of all stakeholders to ensure that we meet mission requirements. C4IT leaders must inspire their workforce and motivate them to grow professionally, contribute wholly, and be creative.
- **Visibility and Transparency:** We believe that all aspects of C4IT management must be visible and transparent to CG-6 system managers, as well as stakeholders, at all times during system planning, development, and support. Visibility and transparency are particularly important to C4IT spending and system performance. To this end, we support a collaborative investment management process that gives the entire organization access to C4IT priority decisions.
- **Guidance:** We believe in establishing guidelines that ensure organizational agility and effective acquisition, application, and management of C4IT systems through a policy and practices framework, and interactions with stakeholder organizations. Our guidelines provide an appropriate level of discipline and structure, and identify the necessary tools to deliver timely and reliable C4IT systems.
- **Optimizing Outcomes:** We believe in leveraging C4IT to accomplish the Coast Guard's missions and deliver superior results. We recognize the extraordinary value of innovation when employees apply an entrepreneurial spirit by using technology as a performance enabler. With this in mind, we established the enterprise architecture (EA), systems development life cycle (SDLC), and investment management processes with maximum flexibility to ensure that technology improves Coast Guard mission and program performance.
- **Partnering to Accomplish the Coast Guard Missions:** We believe that no CG-6 activity can operate in isolation of Coast Guard operational missions and programs. Our success and ability to add value depends upon the ability of CG-6 to embrace, understand, and support enterprise missions and programs. As such, we must collaborate with our stakeholders to ensure that we meet requirements while following the disciplines established to govern C4IT.



# CG-6 GOALS AND OBJECTIVES

## OVERVIEW

The following strategy consists of the goals and objectives that CG-6 plans to accomplish over the next five years. By achieving these goals and objectives, we will realize the Commandant's strategic vision of the future. The goals are purposely broad with the objectives and initiatives focused primarily on a five-year timeframe. Building on the objectives, the CG-6 Performance Plan (Appendix A) identifies specific initiatives that will enable us to achieve the broader goals. Initiatives will be refined as we progress within objectives. As shown in Figure 2, the goals align to five central themes: technology, security, information, governance, and organizational excellence.

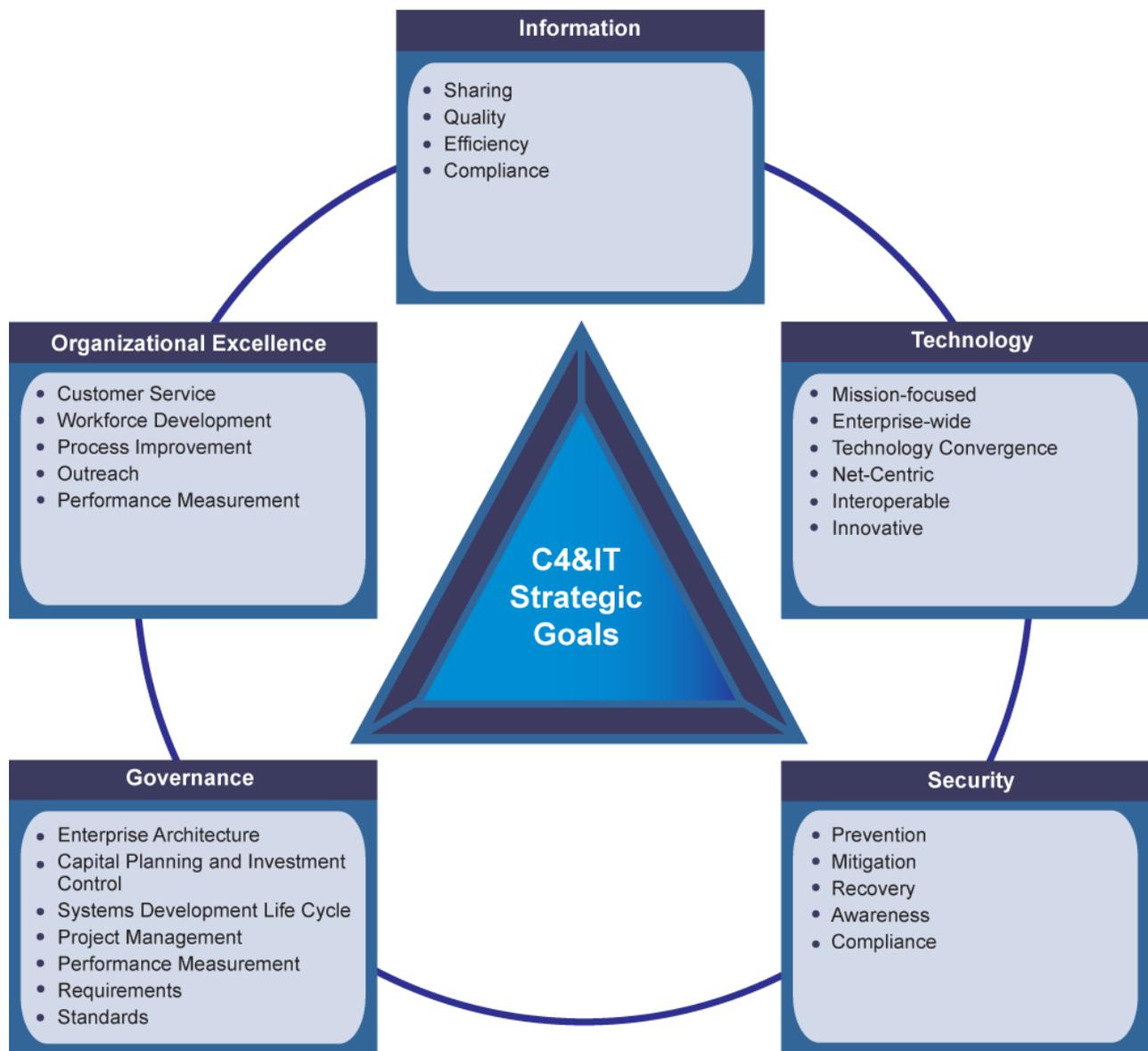


Figure 2: CG-6 Goals Overview



## GOAL 1: INFORMATION

Improve and encourage information sharing, quality, efficiency, and compliance with internal and external partners.

### Intent

Coast Guard mission execution, tactical maneuvers, and command and control depend on our ability to share current and valid information. As such, our personnel must be able to manage the information required to perform their duties and make better decisions. This includes, but is not limited to, tactical, surveillance, law enforcement, financial, and readiness data. In addition, as the Coast Guard becomes more dependent on information sharing, it is increasingly important for us to be able protect information quality and enhance information efficiency. We must also ensure compliance with departmental guidance regarding the protection, transmission, and management of information. This includes the adoption of the National Information Exchange Model (NIEM) and DHS Enterprise Data Management Office (EDMO) practices in support of the DHS Information Sharing Environment. By doing so, we can help to improve mission execution and performance results.

### Objectives

- 1.1 Sharing: Enable information sharing by ensuring that information is visible, understandable, accessible, and interoperable throughout the Coast Guard and with external partners.
- 1.2 Quality: Promote information quality by establishing processes and procedures to make sure that the Coast Guard's information is valid, consistent, and comprehensive.
- 1.3 Efficiency: Provide improved support for the Coast Guard business and mission by ensuring that Coast Guard information is requirements-based, non-duplicative, timely, and financially sound.
- 1.4 Compliance: Achieve the intent of Federal and departmental information management legislation and policies, including compliance with privacy, Freedom Of Information Act (FOIA), and records management guidance.



## GOAL 2: TECHNOLOGY

Deliver mission-focused, interoperable, and innovative C4IT solutions for the enterprise.

### Intent

Coast Guard missions are increasingly dependent on the quality of our technology. Operators and support staff use C4IT solutions throughout the Coast Guard to safeguard our oceans and waterways, enforce maritime laws, and serve our Nation. Interoperable and net-centric solutions allow our operators to communicate seamlessly with internal and external partners such as Federal agencies (including the DoD and its components); state, local, and tribal governments; and intelligence agencies. In addition, during times of war, our ability to transition from governmental responsibilities to defensive capabilities requires optimized and innovative C4IT resources. To satisfy mission demands and operator needs, we must deliver mission-focused and interoperable C4IT using enterprise-wide and net-centric solutions, an optimized infrastructure, and wireless communications.

### Objectives

- 2.1 Mission-focused: Satisfy operator C4IT requirements by delivering mission-focused solutions that improve mission execution and business processes, leverage enterprise solutions, and adhere to the Coast Guard Enterprise Architecture (CGEA).
- 2.2 Enterprise-wide: Define, implement, and enforce standards for supportable and enterprise-wide C4IT systems, applications, products, and standards to enable interoperability, seamless communications, and consolidation.
- 2.3 Technology Convergence: Optimize the Coast Guard C4IT environment and reduce costs of operation by consolidating and integrating infrastructure in alignment with the Department's IT modernization and transition strategy.
- 2.4 Net-Centric: Leverage network technologies to discover and exchange needed information in a timely manner.
- 2.5 Interoperable: Identify and replace stove-piped networks, systems, and applications with C4IT solutions that are interoperable within the Coast Guard and with our partners.
- 2.6 Innovative: Proactively apply innovative technologies and best practices to improve systems, close gaps, and set the pace for Government agencies and industry.



## GOAL 3: SECURITY

Enhance mission effectiveness by preventing C4IT security incidents, such as Cyber attacks and intrusions, and enhancing C4IT security mitigation, awareness, and compliance.

### Intent

As the Coast Guard becomes more dependent on networked communications to accomplish its mission, it is increasingly important to protect the integrity of the network and the information it stores and transmits. As such, any interruption, delay, or degradation in C4IT capabilities can prevent access to critical information and processes. To protect our vital C4IT resources, the Coast Guard must follow best practices, found within industry and Government, to create a layered defense for the systems that the Coast Guard relies on for mission execution. Additionally, we must develop appropriate policies, acquire and field equipment, monitor our networks, train our workforce, and remain vigilant in our efforts to protect and maintain the integrity of the Coast Guard's computer and communication networks. By preventing C4IT security issues and enhancing C4IT security mitigation, recovery, awareness, and compliance, we can support international stability and national defense.

### Objectives

- 3.1 Prevention: Enhance C4IT security by ensuring that proper safeguards and archiving processes are in place to ensure the confidentiality, integrity, availability, and privacy of information and compliance with legal requirements.
- 3.2 Mitigation: Improve the Coast Guard's ability to detect and respond to C4IT security incidents in a timely manner with minimal disruption to systems and the Coast Guard's ability to carry out its missions.
- 3.3 Recovery: Enhance Continuity of Operations Planning (COOP) to respond effectively to security-related threats and natural disasters, and rapidly restore Coast Guard systems and data.
- 3.4 Awareness: Ensure security considerations are at the forefront of all C4IT activities by developing acquisition strategies and guidance to strengthen C4IT security and build compliance.
- 3.5 Compliance: Increase Coast Guard compliance with the Federal Information Security Management Act (FISMA) to ensure that the technologies employed protect sensitive and confidential information, and sustain the privacy of Coast Guard personnel and American citizens.



## GOAL 4: GOVERNANCE

Govern the C4IT enterprise through the execution of technical authority and effective processes for enterprise architecture, capital planning and investment control, systems development, project management, performance measurement and requirements.

### Intent

The fundamental purpose of executing C4IT governance activities within the Coast Guard is to enable the strategic and tactical alignment of C4IT investments, projects, and system development with the Coast Guard's priorities and goals. Using our technical authority we will maximize return on investment, mitigate risk, and ensure business and technical alignment to the CGEA. Effective governance will improve the Coast Guard's ability to meet the cost, schedule, and performance parameters of its C4IT investments.

### Objectives

- 4.1 Enterprise Architecture: Implement an accurate, current, and complete CGEA as the single source of C4IT business and technology information throughout the Coast Guard to improve decision-making.
- 4.2 Capital Planning and Investment Control: Establish effective policies and processes to govern the development and deployment of C4IT throughout the Coast Guard and ensure effective oversight and financial management, and compliance with laws, regulations, and policies.
- 4.3 Systems Development Life Cycle: Facilitate the SDLC process to ensure the collection, validation, and fulfillment of requirements; adherence to the CGEA; and the design and support of comprehensive solutions.
- 4.4 Performance Measurement: Establish relevant and meaningful C4IT performance measures to understand mission execution.
- 4.5 Project Management: Use common and repeatable processes to execute projects that deliver C4IT products and services on time and within budget.
- 4.6 Requirements: Collaborate in the generation of business requirements, and their associated technical requirements, through a disciplined management strategy that establishes policies, practices, and procedures for capturing, storing, and managing all requirements.
- 4.7 Standards: Influence the development of international and industry standards.



## GOAL 5: ORGANIZATIONAL EXCELLENCE

Achieve C4IT organizational excellence by continually developing our workforce, collaborating with internal and external partners, and improving business processes.

### Intent

The Coast Guard depends on its people to perform its mission. Creating an environment that fosters organizational excellence begins with equipping, developing, and preparing our people for personal, professional, and organizational success. We can do this by providing them with the correct education, training, and professional experience needed to achieve C4IT competencies. In addition, we must communicate the value of C4IT and the CG-6 mission, vision, and strategy to enable our people to meet organizational goals. Organizational excellence also requires that processes are continually improved and streamlined to provide efficient and convenient access to C4IT resources. Mission execution is the ultimate goal of organizational excellence.

### Objectives

- 5.1 Customer Service: Provide responsive and effective service by delivering comprehensive, accessible, reliable, and user-friendly solutions to meet or exceed C4IT requirements.
- 5.2 Workforce Development: Equip our people for personal, professional, and organizational success so that we may achieve our mission with a workforce that is trained, prepared, safe, and diverse.
- 5.3 Process Improvement: Establish, institutionalize, and continually update processes to ensure streamlined, integrated, and optimized use of C4IT resources.
- 5.4 Outreach: Communicate the value of C4IT, and the CG-6 mission, vision, and strategy.
- 5.5 Performance Measurement: Use relevant and meaningful C4IT performance measures to understand mission execution.



## THE WAY AHEAD

This strategic plan establishes the goals and objectives for CG-6, and demonstrates how they align with the overall Coast Guard and DHS strategic plans. Supporting this strategy, Appendix A: CG-6 Performance Plan, identifies specific initiatives, milestones, and critical success factors needed to progress toward achieving these goals and objectives.

In essence, the CG-6 Performance Plan is the tactical plan for CG-6. It describes the initiatives that we are executing in support of CG-6 goals. All of the work we do as CG-6 should support one or more of our strategic goals and objectives. As such, all of our major deliverables should fall within the scope of at least one of the initiatives described in the CG-6 Performance Plan. This alignment with the CG-6 strategic goals ensures that we are using our limited resources to satisfy our strategic goals.

We update both the C4IT Strategic Plan and the CG-6 Performance Plan on a yearly basis. The strategic plan contains high-level goals and objectives while the performance plan contains initiatives that we will complete to achieve our goals and objectives. We split multi-year initiatives into milestones to reflect how an initiative will progress over the next five years. More detail is provided for the current fiscal year than for upcoming fiscal years. This ensures that the plan contains sufficient detail to accurately track progress throughout the year.

Our success with completing the milestones documented in this plan will be included as part of an overall CG-6 “dashboard.” We will describe the status of each milestone as “red,” “yellow,” or “green.” Each status will depend on the progress that we are making toward successfully completing the initiative. Green milestones are milestones that were completed on time. Yellow milestones are ones that were completed late or are at risk of being met. Red milestones are milestones from the current fiscal year that were not completed. We will automatically record all incomplete items at the end of the year as “red.”

Together the C4IT Strategic Plan and the CG-6 Performance Plan will provide our CG-6 community with clear direction on our goals and objectives, and a snapshot of our progress toward achieving these goals. Communicating this information to all of CG-6 will help us join together to provide the best possible service to our customers and better align our resources to support the Coast Guard’s mission.





# CG-6 Performance Plan

---

FY11

# APPENDIX A: CG-6 PERFORMANCE PLAN

## INTRODUCTION

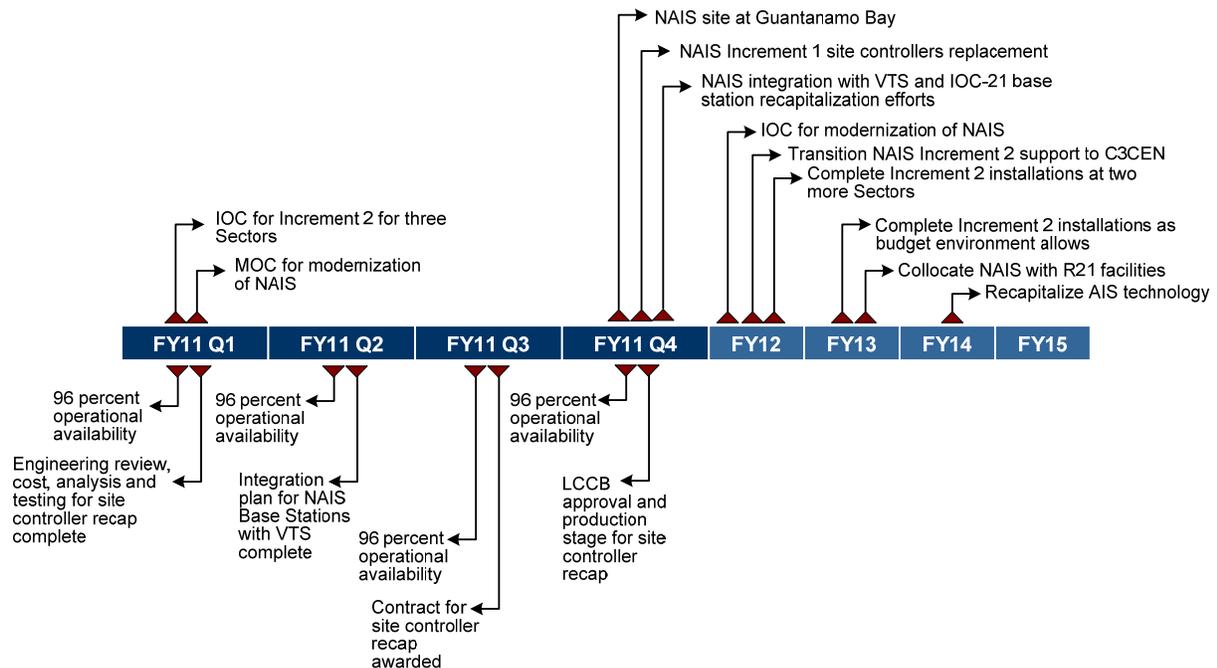
This appendix presents the CG-6 Performance Plan for Fiscal Year 2011 (FY11). The strategic activities presented in this plan and their associated milestones, deliverables and key performance indicators are subject to resource and funding availability. Based on changing requirements and priorities, CG-6 will make trade-off decisions throughout FY11 to effectively manage the Coast Guard's enterprise architecture in a dynamic environment.

## GOAL 1: INFORMATION

### Strategic Activities

#### 1.1 Sharing

- 1.1.1 Nationwide Automated Identification System (NAIS)  
 Exercise technical authority responsibilities in direct support of NAIS to enhance Maritime Domain Awareness (MDA). (Primary Point of Contact (POC): C4IT Service Center/C3CEN; Remote Mission Systems Product Line (RMS-PL))



#### Current Year Milestones

- FY11 Q1: Achieve IOC for Increment 2 for 3 Sectors (CG-933)
- FY11 Q1: Reach Minimum Operating Capability (MOC) for Modernization of NAIS (C3CEN)
- FY11 Q4: Install NAIS Increment 1 Site at Guantanamo Bay (C3CEN)



- FY11 Q4: Replace NAIS Increment 1 Site Controllers (C3CEN)
- FY11 Q4: Integrate NAIS with VTS and IOC-21 base station recapitalization efforts

*Long-term Milestones (Years 2-5)*

- FY12: Reach IOC for Modernization of NAIS Section of the Remote Mission Systems Product Line (C3CEN)
- FY12: Transition NAIS Increment 2 sustainment to C3CEN
- FY12: Complete Increment 2 Installations at 2 additional Sectors (CG-933)
- FY13: Complete NAIS Increment 2 Installations as budget environment allows (CG-933)
- FY13: Collocate NAIS with R21 facilities
- FY14: Recapitalize AIS Base Station technology

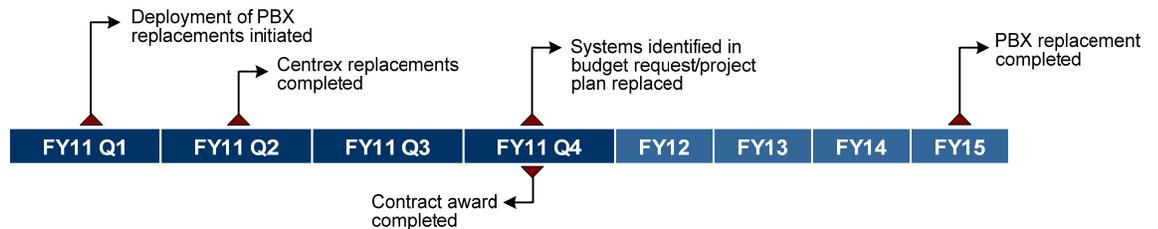
*Critical Success Factors*

- FY11 Q1: Maintain 96 percent operational availability of NAIS (calculated by Sector)
- FY11 Q1: Complete engineering review, cost analysis, and testing for site controller recapitalization
- FY11 Q2: Maintain 96 percent operational availability of NAIS (calculated by Sector)
- FY11 Q2: Complete integration plan for NAIS Base Stations with VTS and IOC-21
- FY11 Q3: Maintain 96 percent operational availability of NAIS calculated by Sector
- FY11 Q3: Contract awarded for the recapitalization of site controllers
- FY11 Q4: Maintain 96 percent operational availability of NAIS (calculated by Sector)
- FY11 Q4: LCCB approval and production stage for NAIS site controller recapitalization



### 1.1.2 Telephony

Develop telephony solutions for the Coast Guard (to include Private Branch Exchange (PBX) replacement, PBX security and unified messaging). (Primary POC: C4IT Service Center/TISCOM)



#### Current Year Milestones

**FY11 Q1:** Begin deployment of PBX replacements including unified messaging where applicable (initially the deployment of UM will be for proof of concept)

**FY11 Q2:** Complete Centrex replacements funded with FY10 fallout

**FY11 Q4:** Replace systems identified in budget request/project plan

#### Long-term Milestones (Years 2-5)

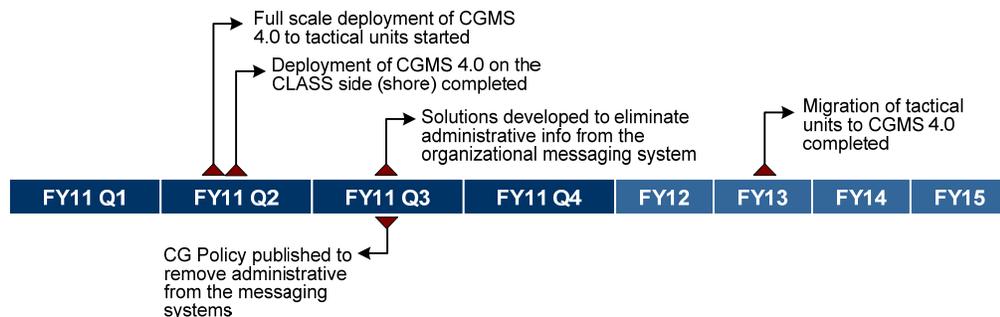
**FY14:** Complete the deployment of PBX replacement

#### Critical Success Factors

**FY10 Q4:** Complete contract award

### 1.1.3 Organizational Messaging Deployment

Deploy the systems necessary to allow the Coast Guard to send, receive and record messages at shore units and mobile units (cutters). The systems must be compatible with DoD and DHS. The organizational messaging community is in a great deal of upheaval at the present and both target architectures and even required capabilities continue to change based on DoD efforts. Our current direction is to migrate the classified and unclassified side to the Coast Guard Messaging System (CGMS) 4.0; and begin to develop solutions to eliminate administrative information from the organizational messaging system. (Primary POC: C4IT Service Center/TISCOM)



#### Current Year Milestones

**FY11 Q2:** Begin full scale deployment of CGMS 4.0 to tactical units

**FY11 Q2:** Finish deployment of CGMS 4.0 on the CLASS side (shore)



FY11 Q4: Develop solutions to eliminate administrative information from the organizational messaging system

*Long-term Milestones (Years 2-5)*

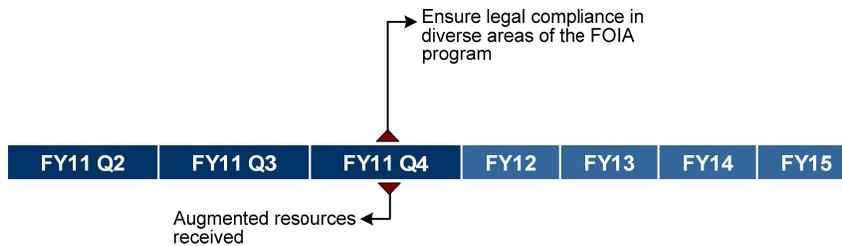
FY13: Complete the migration of tactical units to CGMS 4.0

*Critical Success Factors*

FY11 Q3: CG Policy published to remove administrative traffic from the messaging systems (CG-6 should coordinate)

1.1.4 Freedom of Information Act (FOIA) Compliance

Promulgate policy, educate staff, and monitor responses to ensure Coast Guard compliance with FOIA legislation, regulations, legal precedents and procedures, including processing appeals of adverse decisions to FOIA requests. Address provisions of the Open Government Act by developing a strategy/methodology to measure timeliness and comprehensiveness of responses to FOIA requestors throughout the enterprise using a Coast Guard-wide tracking system, the web and/or social media, and taking into account command reorganizations in response to modernization. (Primary POC: CG-61)



*Current Year Milestones*

FY11 Q4: Ensure legal compliance in diverse areas of the FOIA Program, including with new legislative mandates/Executive Orders while addressing parameters of the Open Government Act such that enterprise-wide data regarding requests is publicly available; appeals are mitigated to the fullest extent; and the Program is supported with an additional 16 billets enterprise-wide needed to perform Program operations

*Long-term Milestones (Years 2-5)*

FY12: Continue milestones outlined for FY11, updating strategies as needed, while working with DHS, OMB, et al to ensure FOIA requests are performed efficiently and comprehensively

FY13-14: Continue milestones outlined for FY11-12, updating strategies as needed, using new technology/processes when feasible to streamline Program operations

*Critical Success Factors*

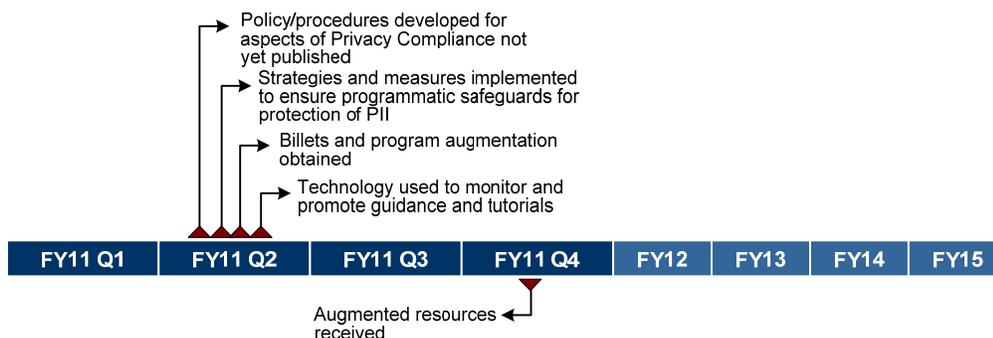
FY11 Q4: Augmented resources received

1.1.5 Privacy Compliance

As a part of managing Personally Identifiable Information (PII) to meet legal



requirements, mitigate risks and conform to provisions of the SDLC, attain Privacy Threshold Analyses (PTAs) for review no later than at the systems' 35 percent design phase. Ensure required compliance documents, including Privacy Impact Assessments (PIAs), System of Record Notices (SORNs) and Notices of Proposed Rulemakings (NPRMs) are consolidated under existing Federal/DHS-wide SORNs or published independently. Update PTAs, PIAs, SORNs and NPRMs for systems significantly changed or amended. (Primary POC: CG-61)



*Current Year Milestones*

- FY11 Q2: In addition to meeting DHS, OMB, and SDLC requirements, develop policy/procedures for myriad aspects of Privacy Compliance not yet published (regarding issues such as the collection/use of PII in diverse venues e.g. social media) by collaborating with Program Managers, Public Affairs, and Legal
- FY11 Q2: Develop strategies and implement measures to ensure programmatic safeguards for protection of PII are established
- FY11 Q2: Obtain billets and program augmentation to perform essential outreach activities
- FY11 Q2: To mitigate risks, use technology and the web (e.g. CG Portal) to monitor and promote guidance and tutorials

*Long-term Milestones (Years 2-5)*

- FY12-14: Continue the many activities outlined for FY11 above

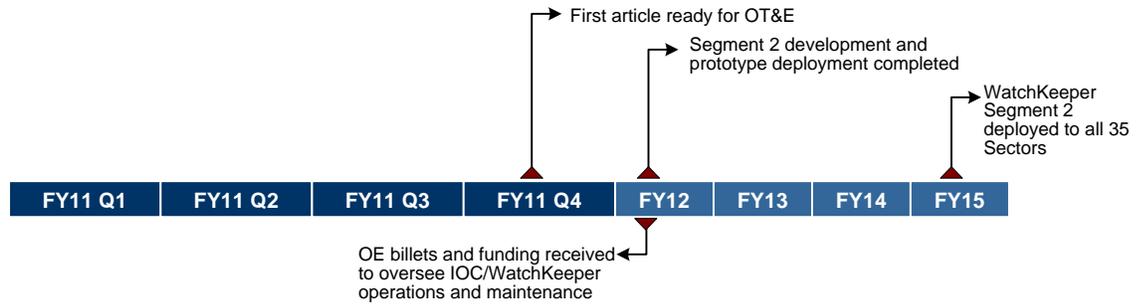
*Critical Success Factors*

- FY11 Q4: Augmented resources received

1.1.6 Interagency Operation Center (IOC)/(WatchKeeper) Delivery

As the principal development agent for CG-9333, develop the first article IOC. The Segment 2 requirement is to consume data from existing sensors into the IOC/WatchKeeper system. (Primary POC: C4IT Service Center/C3CEN/Command Centers)





**Current Year Milestones**

FY11 Q4: Prepare first article for the Operational Test and Evaluation (OT&E)

*Long-term Milestones (Years 2-5)*

FY12: Complete WatchKeeper Segment 2 development and deploy prototype

FY13-15: Deploy WatchKeeper Segment 2 to all 35 Sectors and assist with moves/new builds as funding becomes available

*Critical Success Factors*

FY12 Q2: Receive OE billets and funding to oversee continued IOC/WatchKeeper operations and maintenance

1.1.7

**Strategic Command Center – Global Command & Control System (GCCS) servers**

Replace the GCCS servers at the Coast Guard Atlantic and Pacific Area Command Centers to enable classified and Sensitive But Unclassified (SBU) tactical data exchange with the DoD Commands, including NORTHCOM. This will enable the Common Operating Picture (COP) to be populated with Coast Guard and DHS blue forces, normal maritime surface and air traffic, and targets of interest. ( Primary POC: C4IT Service Center/C3CEN)



*Current Year Milestones*

FY11 Q2: Achieve full sustainment of GCCS-J with migration toward the next generation command and control system

*Long-term Milestones (Years 2-5)*

FY11-14: Achieve full sustainment of GCCS-J with migration toward the next generation command and control system

*Critical Success Factors*

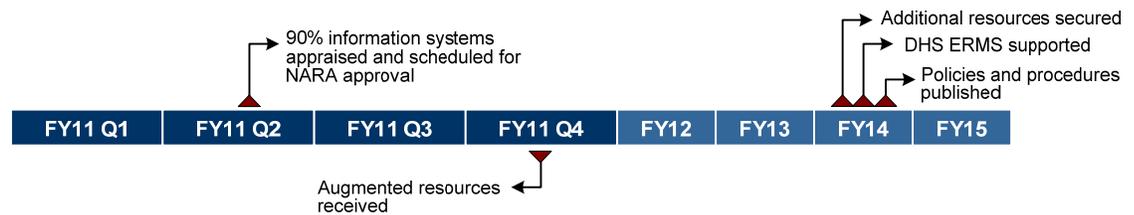
FY11 Q3: Develop and agree upon new architecture that reduces hardware in field while increasing data sharing

1.2 Quality



### 1.2.1 Data Stewardship

Data stewardship encompasses the overall management of Information, from creation through disposition. The Coast Guard promulgates policies and procedures to ensure data is properly collected used, maintained, stored and shared to meet legal requirements. Key elements of this stewardship involve parameters of the Records Management Program, which requires appraising/scheduling systems and other agency records regardless of media for determination of retention requirements, thus protecting the agency' legal, financial, operational and historic interests. Trustworthiness of records ensures their admissibility in court under the Federal Rules of Evidence and assists in successful discovery results during litigation. Acquisition of an electronic recordkeeping system in conformance with the Coast Guard Enterprise Architecture (CGEA) would ensure long term readability/usability of agency records meeting requirements of the National Archives and Records Administration (NARA) and other legal mandates. As such, working with the Department to plan, test and ultimately implement DHS' Electronic Records Management System (ERMS) will provide the Coast Guard with an essential asset, which will require additional funding. (Primary POC: CG-61)



#### *Current Year Milestones*

FY11 Q4: Appraise and schedule ninety percent of information systems for approval by the National Archives and Records Administration (NARA)

#### *Long-term Milestones (Years 2-5)*

FY12-14: As Records Management Program mandates are growing exponentially, secure additional resources needed to manage agency-wide transactions, while ensuring data/records management processes meet SDLC, EA, NARA and DHS requirements

FY12-14: Continue all strategic activities outlined above and actively participate with the Department's ERMS project to support acquisition and implementation of a uniform electronic recordkeeping system

FY12-14: Continue to publish policies and procedures as required

#### *Critical Success Factors*

FY11 Q4: Augmented resources received

### 1.3 Efficiency

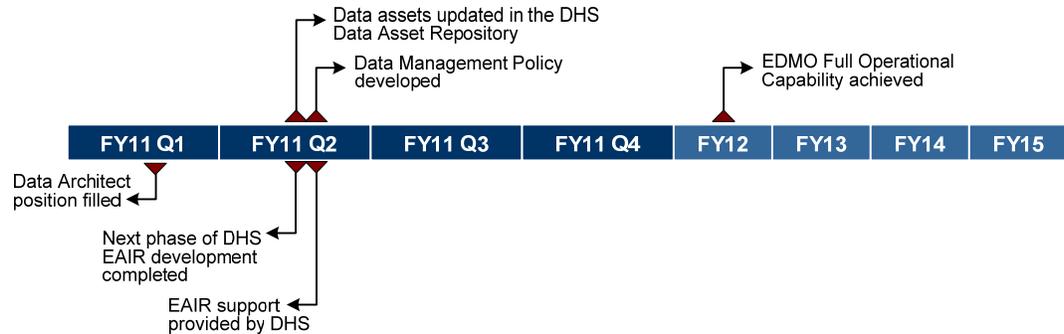
See initiative 1.4.1.

### 1.4 Compliance



#### 1.4.1 Enterprise Data Management Office (EDMO)

Increase the efforts of the Coast Guard Enterprise Data Management Office (EDMO). This includes documenting the Coast Guard's data assets and establishing the principles, policies and practices necessary for Coast Guard information sharing, quality, efficiency and compliance. (Primary POC: CG-66)



##### *Current Year Milestones*

- FY11 Q3: Update the data assets in the DHS Data Asset Repository to address the five new attributes
- FY11 Q3: Develop a Data Management Policy

##### *Long-term Milestones (Years 2-5)*

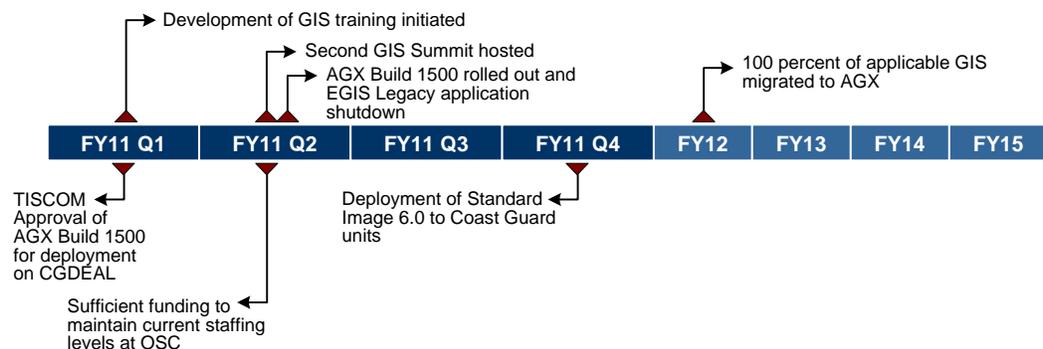
- FY12: Achieve full operating capability for the Coast Guard EDMO

##### *Critical Success Factors*

- FY11 Q1: Data Architect position filled
- FY11 Q2: Next phase of DHS EAIR development completed
- FY11 Q2: EAIR population and maintenance support provided by DHS

#### 1.4.2 Geospatial Management Office (GMO)

Increase efforts for the Coast Guard Enterprise Geospatial Management Office (GMO). This includes establishing a single enterprise GIS solution and migrating redundant systems to the enterprise solution. (Primary POC: CG-63)



##### *Current Year Milestones*

- FY11 Q1: Initiate development of GIS training
- FY11 Q2: Host the second GIS Summit



- FY11 Q2: Roll out AGX Build 1500 and shutdown EGIS Legacy application
- FY11 Q4: Migrate 50 percent of the GIS identified for migration to AGX

*Long-term Milestones (Years 2-5)*

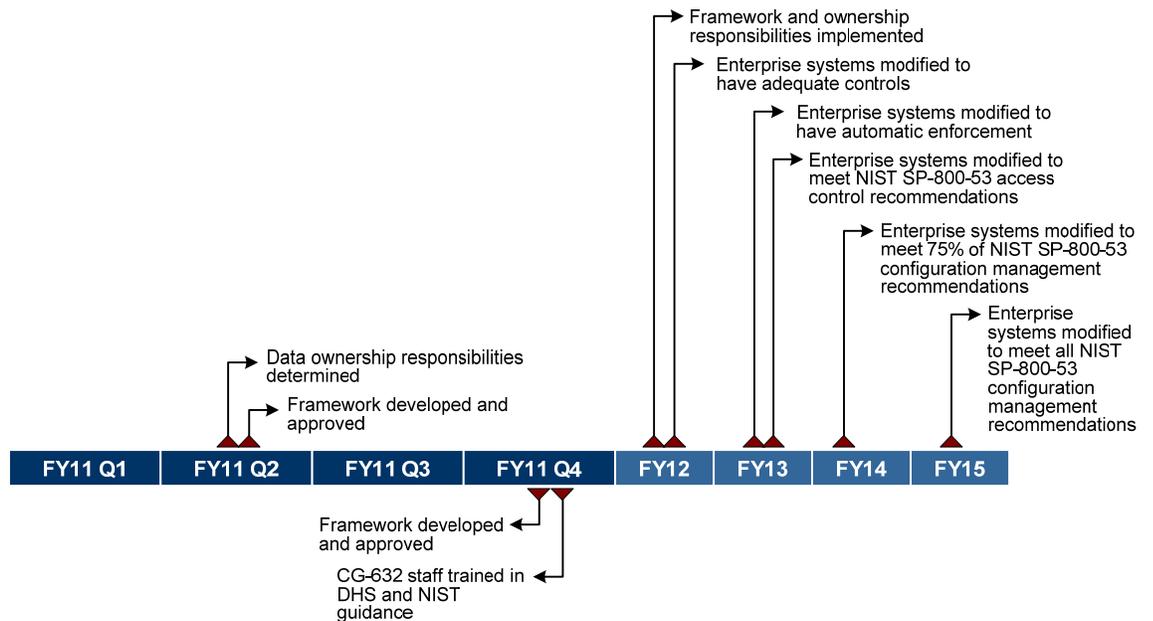
- FY12: Migrate 100 percent of the GIS identified for migration to AGX

*Critical Success Factors*

- FY11 Q1: TISCOM Approval of AGX Build 1500 for deployment on CGDEAL
- FY11 Q2: Sufficient funding to maintain current staffing levels at OSC
- FY11 Q4: Deployment of Standard Image 6.0 to Coast Guard units

1.4.3 Data and System Controls Ownership

Establish business unit responsibility and ownership of financial and production data and related system controls. As part of this effort, CG-6 will leverage DHS guidance, including the C&A framework, and departmental guidance, including the OMB Circular A-123 compliance activities. (Primary POC: CG-63)



*Current Year Milestones*

- FY11 Q4: Work with CG-8 and determine which business function is ultimately responsible for each piece of data
- FY11 Q4: Finish the development and get approval for the framework

*Long-term Milestones (Years 2-5)*

- FY12: Implement the agreed to framework and ownership roles/responsibilities
- FY12: Modify enterprise systems to have adequate controls to make sure that users have access rights consistent with their roles



- FY13: Modify enterprise systems to have automatic enforcement of appropriate password strength or adequate administrative controls to compensate
- FY13: Modify enterprise systems to meet National Institute of Standards and Technology (NIST) SP-800-53 recommendations for access control
- FY14: Modify enterprise systems to meet 75 percent of NIST SP-800-53 recommendations for configuration management
- FY15: Modify enterprise systems to meet all NIST SP-800-53 recommendations for configuration management

*Critical Success Factors*

- FY11 Q4: Framework developed and agreed upon by owners and stakeholders
- FY11 Q4: CG-632 staff trained in DHS and NIST guidance



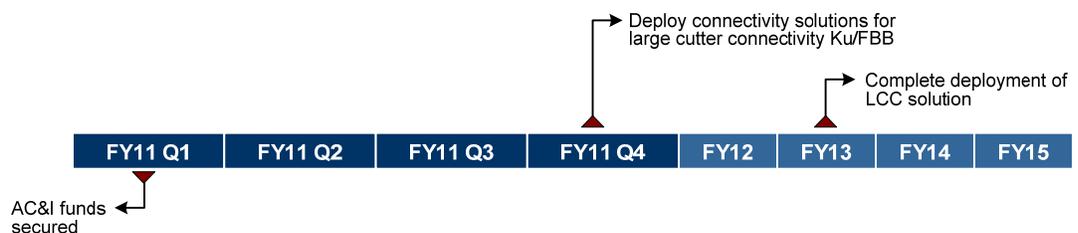
## GOAL 2: TECHNOLOGY

### Strategic Activities

#### 2.1 Mission-Focused

##### 2.1.1 Large Cutter Connectivity

Deploy internet protocol connectivity solutions using commercial satellite communications technology to improve performance, increase bandwidth, and lower costs for capital cutters (WMEC, HEC, MSL, etc.) and deployable units. (Primary POC: C4IT Service Center/TISCOM; Network Infrastructure Product Line (NI-PL))



##### *Current Year Milestones*

FY11 Q4: Deploy connectivity solutions for large cutter connectivity Ku/FBB (priority going to NSCs, 378s, and Able Lookout 270s)

##### *Long-term Milestones (Years 2-5)*

FY12: Complete deployment of LCC solution (up to 20 additional cutters) including the WMEC Mature, WAGB 399, WPC 179, WAGB 420, and WIX 327

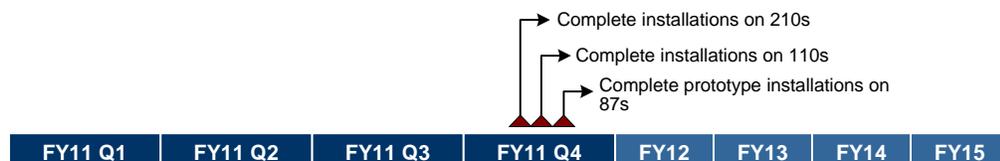
##### *Critical Success Factors*

FY10 Q4: Contract award completed

FY11 Q1: AC&I funds secured for FY11 efforts

##### 2.1.2 Small Cutter Connectivity

Deploy internet protocol connectivity solutions to improve performance, increase bandwidth and lower costs for cutters not covered in the large cutter connectivity effort. (Primary POC: C4IT Service Center/TISCOM)



##### *Current Year Milestones*

FY11 Q4: Complete installations on 210s

FY11 Q4: Complete installations on 110s



FY11 Q4: Complete prototype installations on 87s

*Long-term Milestones (Years 2-5)*

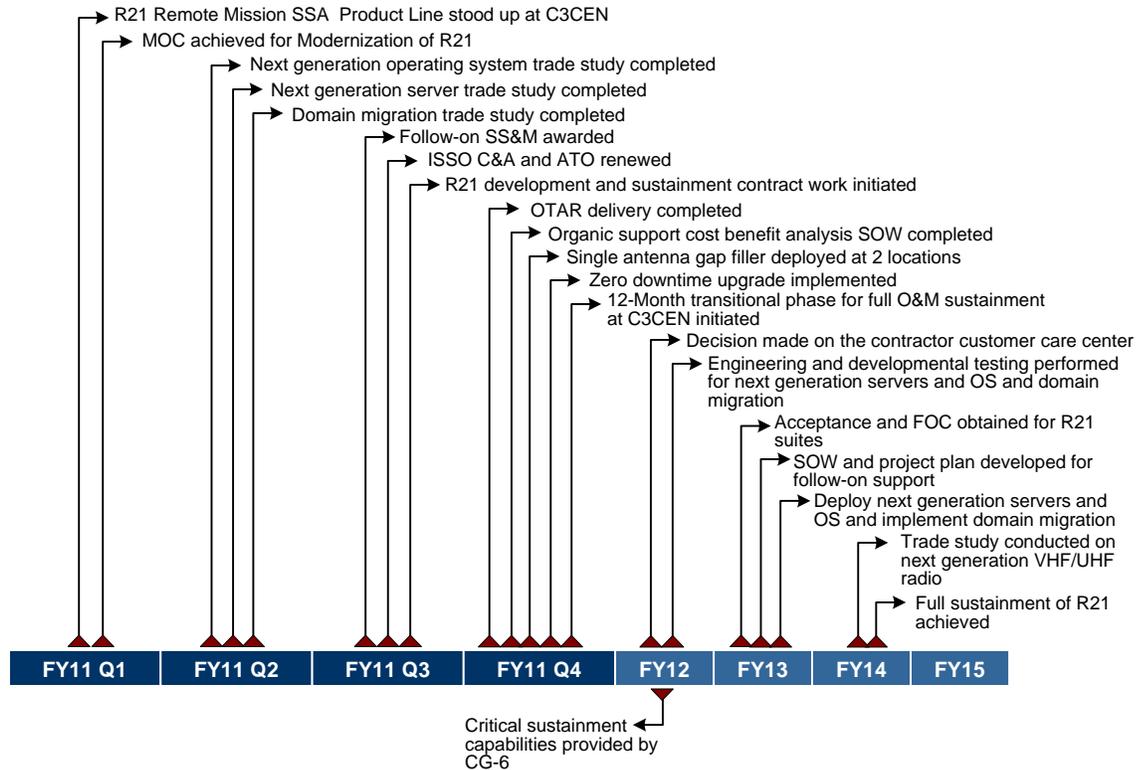
There are no long-term milestones for this initiative.

*Critical Success Factors*

FY10 Q4: Contract award completed

2.1.3 Rescue 21 Life Cycle Management Transition

Transition Rescue 21 assets from acquisition to sustainment. (Primary POC: CG-64)



*Current Year Milestones*

FY11 Q1: Stand-up Rescue 21 Remote Mission System Support Agent (SSA) responsibilities(RMS) Product Line at C3CEN

FY11 Q1: Reach Minimum Operating Capability (MOC) for Modernization of R21 (C3CEN)

FY11 Q2: Complete Next Generation Operating System Trade Study (CG-933)

FY11 Q2: Complete next generation server trade study (CG-933)

FY11 Q2: Complete domain migration trade study (CG-933)

FY11 Q3: Award follow-on (CY12 – CY15) system, support, and maintenance (SS&M) contract (CG-933)

FY11 Q3: Complete ISSO re-certification and re-accreditation and renew Authority to Operate (ATO) for R21 (CG-933 & C3CEN)



- FY11 Q3: Initiate development of Rescue 21 full and open competitive sustainment contract work
- FY11 Q4: Complete OTAR delivery via R21 towers system wide
- FY11 Q4: Conduct organic support cost benefit analysis statement of work to evaluate existing commercial system support and maintenance contract
- FY11 Q4: Deploy single antenna gap filler at two locations (CG-933)
- FY11 Q4: Implement zero downtime upgrade (CG-933)
- FY11 Q4: Initiate 12-Month transitional phase for full O&M sustainment at C3CEN (R21 FOC expected FY13 Q2)

*Long-term Milestones (Years 2-5)*

- FY12: Assess and decide if the contractor customer care center should be organically supported within the Coast Guard
- FY12: Perform engineering and developmental testing for next generation servers (CG-933)
- FY12: Perform engineering and developmental testing for next generation operating system (OS) (CG-933)
- FY12: Perform engineering and developmental testing of domain migration
- FY13: Obtain acceptance and FOC for Rescue 21 suites at all sectors
- FY13: Prepare statement of work (SOW) and develop project plan for follow-on system support contract (CY16 and beyond) or Resource Proposals for organic support (C3CEN/C4ITSC(COCO))
- FY13: Receive CCB approval and deploy next generation operating system (C3CEN)
- FY13: Receive CCB approval and deploy next generation servers (C3CEN)
- FY13: Receive CCB approval and implement domain migration strategy (C3CEN)
- FY14: Perform trade study on next generation VHF/UHF radio (Quantar replacement) (C3CEN)
- FY14: Achieve full Sustainment of R21

*Critical Success Factors*

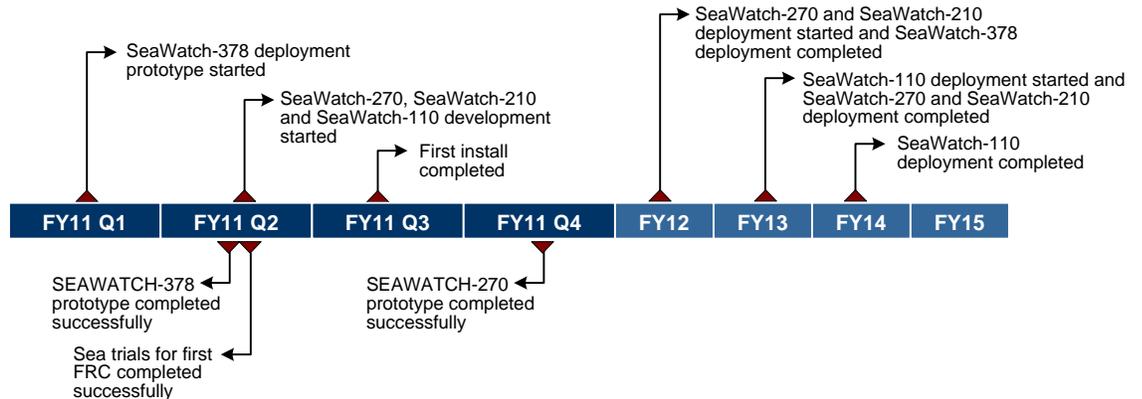
- FY12 Q1: Critical sustainment capabilities provided by CG-6 (enterprises must choose between in-house or outsourcing O&M services to a reliable provider)

2.1.4 SeaWatch-Sentinel Development

As primary development agent for CG-936, develop the Command and Control (C2) system for Sentinel Class patrol boats to be delivered as Government Furnished Information (GFI) to Bollinger Shipyards, Inc. This system will be prototyped on a CG 210 WMEC before delivery as GFI to Bollinger. As System Support Agent/System Development Agent for the Shipboard Command and Control System (SCCS), develop and deploy SeaWatch to replace SCCS currently installed on



WHEC/WMEC/CPB class cutters. (Primary POC: C4IT Service Center/C3CEN; Command & Control Core Technology (C2-CT))



*Current Year Milestones*

- FY11 Q1: Begin SeaWatch-378 deployment prototype
- FY11 Q2: Begin SeaWatch-270, SeaWatch-210 and SeaWatch-110 development
- FY11 Q3: Complete the first install

*Long-term Milestones (Years 2-5)*

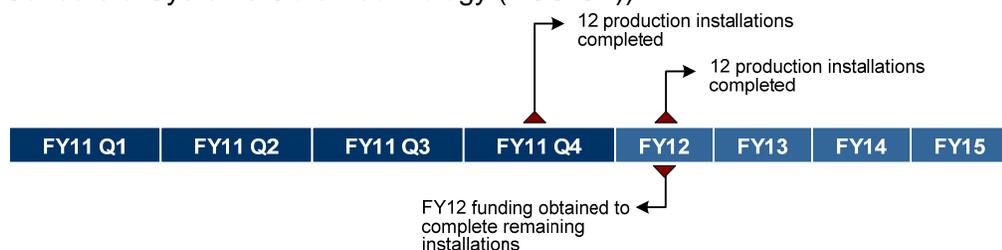
- FY12: Begin SeaWatch-270 and SeaWatch-210 deployment and complete SeaWatch-378 deployment
- FY13: Begin SeaWatch-110 deployment and complete SeaWatch-270 and SeaWatch-210 deployment
- FY14: Complete SeaWatch-110 deployment

*Critical Success Factors*

- FY11 Q2: SEAWATCH-378 prototype completed successfully
- FY11 Q2: Sea trials for first FRC completed successfully
- FY11 Q4: SEAWATCH-270 prototype completed successfully

2.1.5 Buoy Tender Data Distribution System Replacement

Deploy a replacement data distribution system on oceangoing and coastal buoy tenders (WLB/WLM). (Primary POC: C4IT Service Center/C3CEN; Navigation Sensors & Systems Core Technology (NSS-CT))



*Current Year Milestones*

- FY11 Q4: Complete 12 production installations



*Long-term Milestones (Years 2-5)*

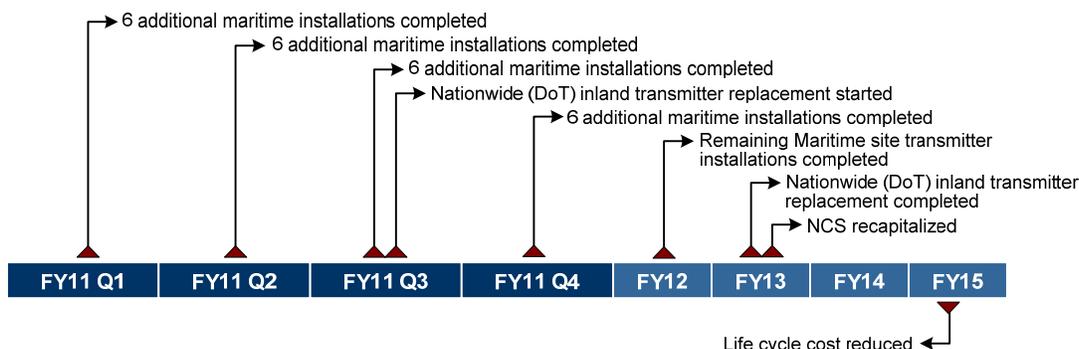
FY12: Complete 12 production installations

*Critical Success Factors*

FY11 Q4: Obtain sufficient funding for FY12 to complete remaining 12 installations in FY12

2.1.6 Differential Global Positioning System (DGPS) Transmitter Replacement

Deploy a replacement transmitter for maritime DGPS sites to provide precise navigation information to the maritime public. (Primary POC: C4IT Service Center/C3CEN/DGPS Product Line (DGPS-PL))



*Current Year Milestones*

- FY11 Q1: Complete 6 additional maritime installations
- FY11 Q2: Complete 6 additional maritime installations
- FY11 Q3: Complete 6 additional maritime installations
- FY11 Q4: Commence Nationwide (DoT) inland transmitter replacement if contract in place
- FY11 Q4: Complete 6 additional maritime installations
- FY11 Q4: Continue Nationwide (DoT) inland transmitter replacement

*Long-term Milestones (Years 2-5)*

- FY12: Complete any remaining Maritime site transmitter installations
- FY12-13: Complete Nationwide (DoT) inland transmitter replacement (expect to receive 5 million dollars funding for inland DGPS sites in the next 2 fiscal years)
- FY12-13: Recap Nationwide Control Station (NCS) based on enterprise Command & Control (C2) and GIS Architecture

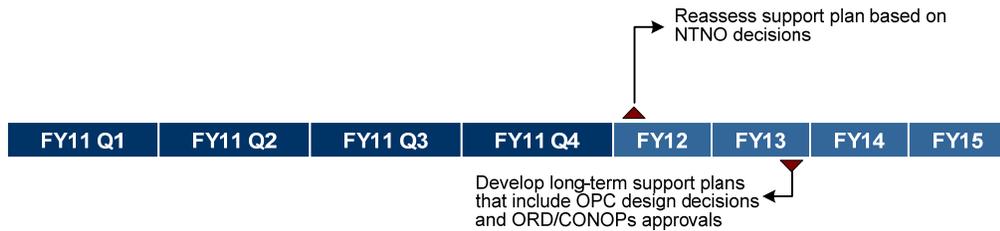
*Critical Success Factors*

FY12-15: Reducing overall lifecycle cost by reducing number of end of lifecycle transmitters in the field

2.1.7 Cutter Sensitive Compartmented Information Facility (SCIF)/ Temporary SCIF (T-SCIF) Capabilities



Initiate efforts to deploy, operate, and sustain SCIF and T-SCIF capabilities.  
 (Primary POC: CG-64)



*Current Year Milestones*  
 None identified.

*Long-term Milestones (Years 2-5)*

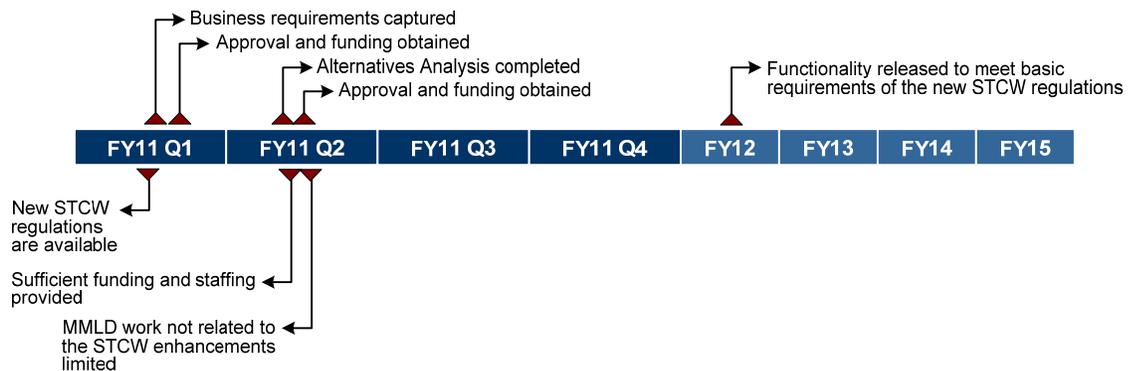
FY12: Reassess support plan based on NTNO decisions

FY13: Develop long-term support plans that include OPC design decisions and ORD/CONOPs approvals

*Critical Success Factors*  
 None identified.

2.1.8 MMLD Modernization

Make enhancements to the MMLD system to address the requirements of the revised STCW regulations and the resulting changes to NMC and REC business processes. (Primary POC: C4IT Service Center/OSC)



*Current Year Milestones*

FY11 Q1: Capture business requirements for STCW regulation impacts and Modernization goals; exam generation, test delivery, scoring, and test results capture and analysis capability for remaining business areas

FY11 Q1: Obtain approval and funding (Development and Recurring O&M) for the Modernization Project; exam generation, delivery, scoring, and results capture and analysis capability

FY11 Q2: Complete the Alternatives Analysis; exam generation, delivery, scoring, and results capture and analysis capability for remaining business areas



FY11 Q2: Obtain approval and funding (Development and Recurring O&M) for the Modernization Project; exam generation, delivery, scoring, and results capture and analysis for remaining business areas

*Long-term Milestones (Years 2-5)*

FY12: Release functionality to meet basic requirements of the new STCW regulations

*Critical Success Factors*

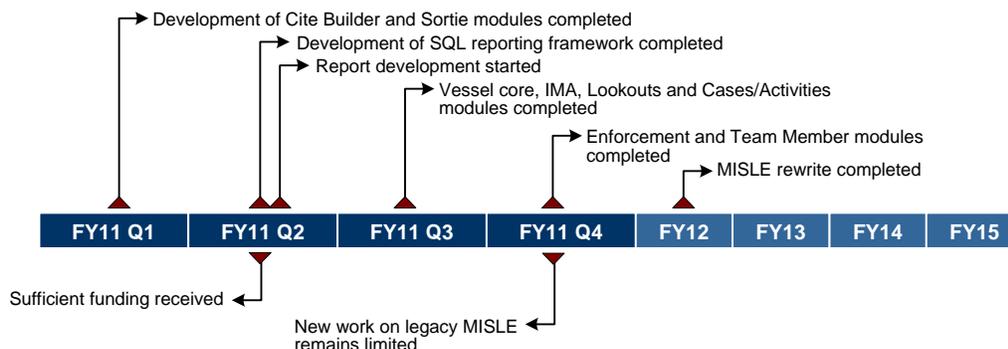
FY11 Q1: New STCW regulations are available

FY11 Q2: Sufficient funding and staffing are provided to implement project plan

FY11 Q2: MMLD work not related to the STCW enhancements will be limited

2.1.9 MISLE Modernization

Rewrite the MISLE system user interface and database to address functionality, security and supportability issues stemming from the existing MISLE software. Intent is to replace current MISLE functionality plus add a limited number of functionality items identified by the MISLE CCB. (Primary POC: C4IT Service Center/OSC)



*Current Year Milestones*

FY11 Q1: Complete development of Cite Builder and Sortie modules

FY11 Q2: Complete development of SQL reporting framework

FY11 Q2: Begin developing reports within MISLE 5.0

FY11 Q3: Complete development of Vessel core, IMA, Lookouts and Cases/Activities modules

FY11 Q4: Complete development of Enforcement and Team Member modules

*Long-term Milestones (Years 2-5)*

FY12: Complete MISLE Rewrite

*Critical Success Factors*

FY11 Q2: Receipt of sufficient funding to maintain current OSC MISLE project staffing levels

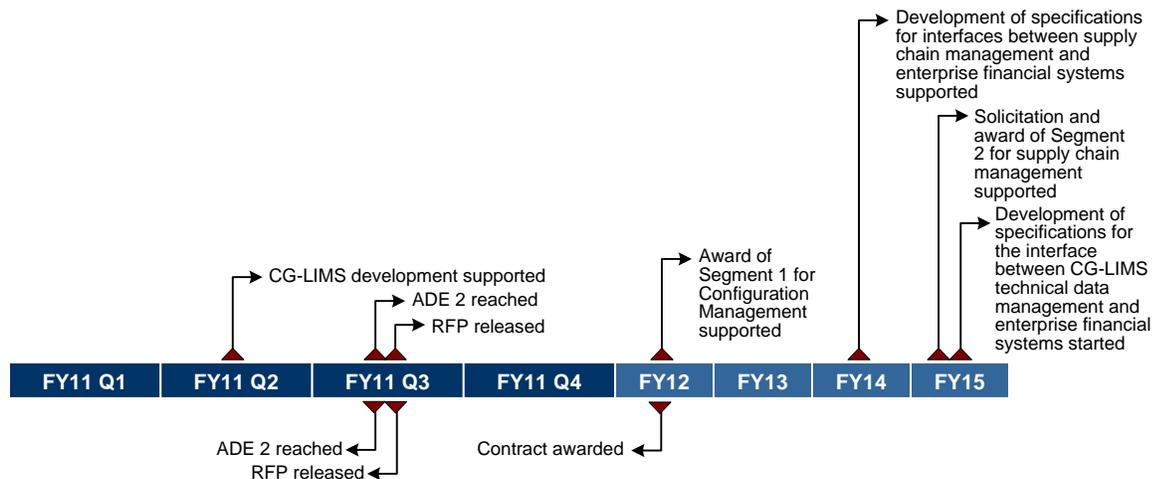


FY11 Q4: New work on legacy MISLE remains limited and does not require the use of resources dedicated to the rewrite outside planned legacy MISLE work sprints

## 2.2 Enterprise-wide

### 2.2.1 Logistics Systems Modernization

Continue to develop the Coast Guard Logistics Information Management System (CG-LIMS) to transform the Coast Guard's logistics systems in support of a Coast Guard-wide, common logistics business model. (Primary POC: CG-63)



#### Current Year Milestones

FY11 Q2: Continue to support CG-4 and CG-9 with the development of specifications for interface between CG-LIMS Configuration Management and enterprise financial systems

FY11 Q3: Reach Acquisition Decision Event (ADE) 2

FY11 Q3: Release the Request for Proposal (RFP)

#### Long-term Milestones (Years 2-5)

FY12: Support CG-4 and CG-9 in the solicitation and award of Segment 1 for Configuration Management, providing input so that CG-LIMS interfaces smoothly with existing financial and mixed systems

FY12-14: Continue to support CG-4 and CG-9 to develop specifications for interface between CG-LIMS Supply Chain Management and enterprise financial systems

FY14-15: Support CG-4 and CG-9 in the solicitation and award of Segment 2 for supply chain management, providing input so that CG-LIMS interfaces smoothly with existing financial and mixed systems

FY15: Begin developing specifications for the interface between CG-LIMS Technical Data Management and enterprise financial systems

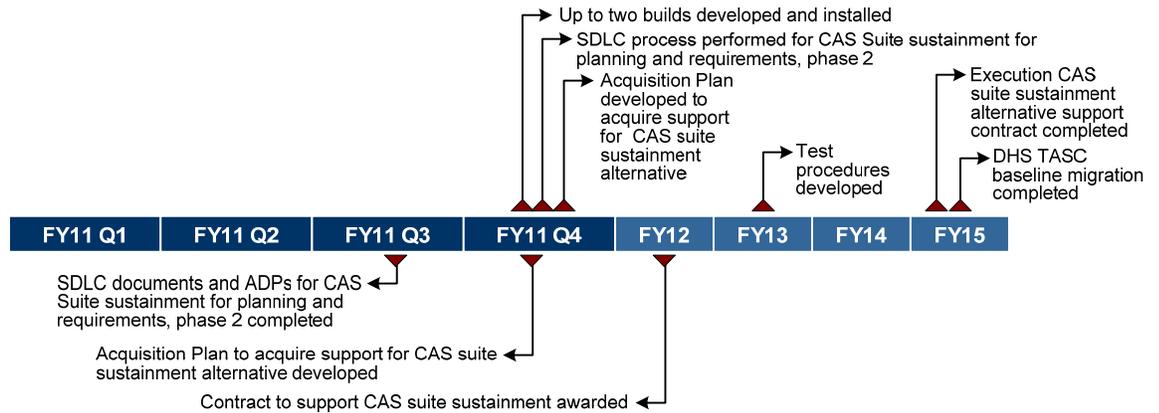


*Critical Success Factors*

- FY11 Q3: Acquisition Decision Event 2 achieved
- FY11 Q3: Request for proposal (RFP) for Segment One Configuration Management released
- FY12 Q3: Contract awarded

2.2.2 Financial Systems Modernization

Support the Coast Guard's financial systems modernization effort to ensure that the Coast Guard's financial systems comply with government accounting, auditing and financial reporting regulations. (Primary POC: CG-63)



*Current Year Milestones*

- FY11 Q4: Develop and install up to two builds
- FY11 Q4: Perform SDLC process for CAS Suite sustainment for planning and requirements, phase 2
- FY11 Q4: Develop Acquisition Plan to acquire support for chosen CAS suite sustainment alternative

*Long-term Milestones (Years 2-5)*

- FY12-15: Execute support contract for chosen CAS suite sustainment alternative
- FY13: Develop test procedures
- FY15: Prepare for and migrate to DHS TASC Baseline

*Critical Success Factors*

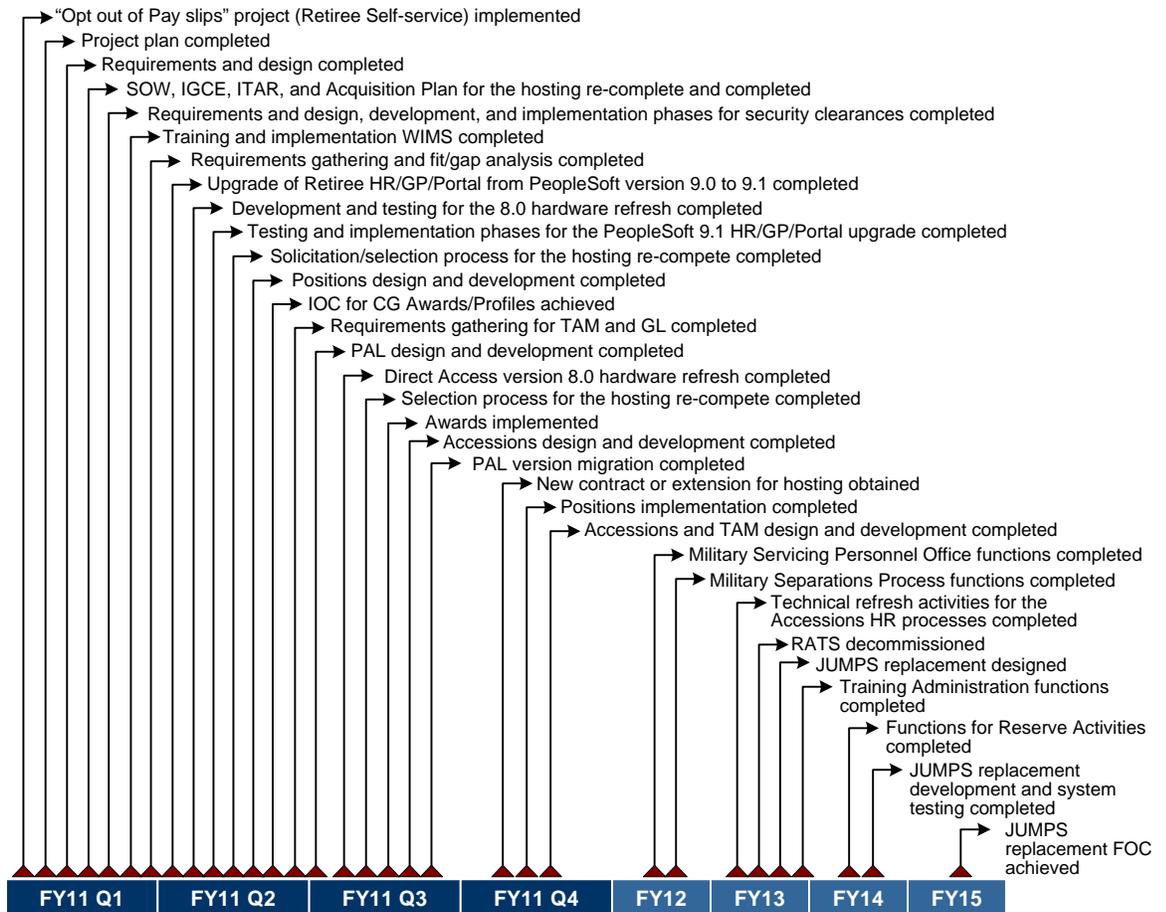
- FY11 Q3: SDLC documents and ADPs for CAS Suite sustainment for planning and requirements, phase 2 completed
- FY11 Q4: Acquisition Plan to acquire support for chosen CAS suite sustainment alternative developed
- FY12 Q1: Contract to support CAS suite sustainment awarded

2.2.3 Military Human Resources (HR)/Payroll Modernization

Continue HR line of business modernization through system development, maintenance and stewardship of the HR applications. Using the Coast Guard SDLC



practices, continue to implement and upgrade Direct Access and PeopleSoft's Global Payroll Application to transform the Coast Guard's Military HR and payroll systems in support of a Coast Guard-wide consolidated Human Resources Management System (HRMS). (Primary POC: CG-63)



*Current Year Milestones*

- FY11 Q1: Implement the “Opt out of Pay slips” project (Retiree Self-service)
- FY11 Q1: Initiate the Requirements gathering phase and complete the design of the project plan with the vendor for the 8.0 hardware refresh
- FY11 Q1: Complete the requirements and design, develop and start the testing phase for the 9.1 HR/GP/Portal upgrade
- FY11 Q1: Complete the Statement of Work (SOW), Independent Government Cost Estimate (IGCE), IT Acquisition Review (ITAR), and Acquisition Plan for the hosting re-complete and submit to DHS and CG to start the process
- FY11 Q1: Complete the requirements and design, development and implementation phases for security clearances (part of the Direct Access 8.0 to 9.1 technical refresh project)



- FY11 Q1: Complete training and implement WIMS (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q1: Initiate requirements gathering process for Accessions (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q1: Start the requirements gathering process for GL (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q1: Initiate the requirements gathering process for PAL (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q1: Start Design and Development phase to PHS with the capability to manage individual job positions (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q1: Complete Requirements gathering and Fit/Gap analysis and start the Design and Development phase for awards (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q2: Complete version upgrade of Retiree HR/GP/Portal from PeopleSoft version 9.0 to 9.1
- FY11 Q2: Complete development and testing for the 8.0 hardware refresh
- FY11 Q2: Complete testing and implementation phases for the PeopleSoft 9.1 HR/GP/Portal upgrade
- FY11 Q2: Complete the solicitation/selection process for the hosting re-compete
- FY11 Q2: Complete Positions design and development, and start testing and training (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q2: Achieve IOC for CG Awards/Profiles, complete development and testing, and start deployment (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q2: Complete Accessions and Talent Acquisition Manager (TAM) requirements gathering for CG and PHS (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q2: Complete the requirements gathering for GL (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q2: Complete CG Personnel Allowance List (PAL) design and development, and start testing (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q3: Complete Direct Access version 8.0 hardware refresh
- FY 11 Q3: Complete selection process for the hosting re-compete
- FY11 Q3: Start Positions Deployment for PHS (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q3: Complete Awards implementation (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q3: Complete Accessions design and development (part of the Direct Access 8.0 to 9.1 technical refresh project)



- FY11 Q3: Complete migration of PAL from version 8.0 to version 9.1 (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q3: Initiate requirements gathering and fit/gap for the Military HR Separations processes (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q4: Obtain a new contract or extension for hosting
- FY11 Q4: Complete Positions implementation (part of the Direct Access 8.0 to 9.1 technical refresh project)
- FY11 Q4: Complete Accessions and TAM design and development for CG and PHS and start the Testing phase (part of the Direct Access 8.0 to 9.1 technical refresh project)

*Long-term Milestones (Years 2-5)*

- FY12: Complete Military Servicing Personnel Office functions (Administration of Travel Orders, Personnel Departing, Personnel Reporting, Entitlement start and stop) migration from version 8.0 to version 9.1
- FY12: Complete Military Separations Process functions (Statement of Intent, Release from AD, Discharge, Retirement including Ret Auth, DD214, Orders, Accounting) migration from version 8.0 to version 9.1
- FY12: Initiate technical refresh activities for the Reserve Activities HR Processes
- FY13: Complete technical refresh activities for the Accessions HR Processes
- FY13: Achieve TAM FOC in PeopleSoft version 9.1.
- FY13: Decommission custom recruiting application RATS
- FY13: Initiate technical refresh activities for the Training Administration HR Processes
- FY13: Initiate technical refresh activities for the Career Management HR Processes
- FY13: Complete Military Payroll (JUMPS replacement) design
- FY13: Complete Training Administration functions (Course/Session Administration, Student Enrollment, Orders Management, Accounting) migration from version 8.0 to version 9.1
- FY14: Complete Reserve Activities functions (Drills, Annual Screen Questionnaire, Reserve Orders, Status Change, Member Training Rating, Montgomery GI Bill, Mobilization/Readiness and Tracking, Defense Manpower Data Center files, Accounting Functions, Demobilization) migration from version 8.0 to version 9.1
- FY14: Complete Military Payroll (JUMPS replacement) development and system testing
- FY14: Initiate technical refresh activities for the Employee Reviews HR Processes
- FY14: Initiate technical refresh activities for the Assignments HR Processes



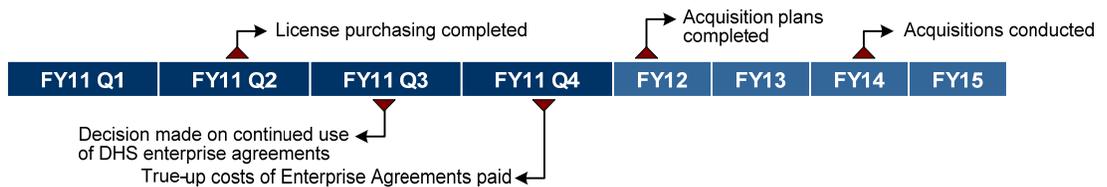
FY15: Achieve FOC for the JUMPS payroll replacement (PeopleSoft HRMS version 9.x, including Global Pay, military payroll subsidiary ledger and internal controls)

*Critical Success Factors*

- Ongoing Earned value management reporting (including project status reports and project work breakdown structure) (monthly)
- Ongoing Enterprise Architecture Board (EAB) and CIO Asset Manager reviews (as needed)
- Ongoing Timely status reports from the contractor and project leads (monthly)
- Ongoing Continued executive sponsorship/direction (including uninterrupted funding and personnel resources)
- Ongoing Completion and formal signoff of system, integration, regression, and user acceptance testing (as needed)
- Ongoing Adherence to SDLC process including artifacts completed or updated as required (as needed)
- Ongoing Timely completion of FISMA compliance artifacts (annually)
- Ongoing Receipt of annual funding from CG and PHS appropriations (Q1 of every FY)

2.2.4 DHS Enterprise Contract Vehicles and License Agreements

Leverage DHS enterprise contract vehicles and enterprise license agreements to reduce costs and meet DHS and Coast Guard product standards. (Primary POC: CG-64 and the C4IT Service Center/TISCOM)



*Current Year Milestones*

FY11 Q2: Complete licensing purchase with true-ups

*Long-term Milestones (Years 2-5)*

FY12: Develop acquisition plans for feasible enterprise agreements

FY13-14: Conduct acquisitions with Coast Guard and/or DHS Contracting offices for identified enterprise agreements

*Critical Success Factors*

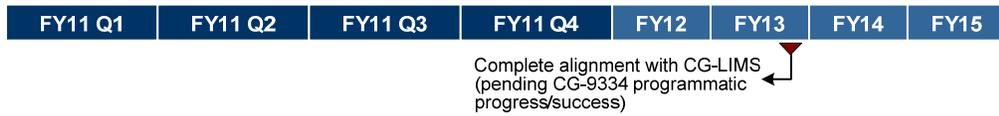
FY11 Q3: Determine if we continue to use the DHS agreements when they increase our costs

FY11 Q4: Pay true-up costs of Enterprise Agreements (if the number of licenses has increased)

2.2.5 Electronic Product Lines Modernization



Standardize all Command, Control, Communications, Combat, Computing, Intelligence, Surveillance, and Reconnaissance (C5ISR) systems maintenance in alignment with the product line model, including the use of ALMIS. (Primary POC: C4IT Service Center)



*Current Year Milestones*  
None Identified.

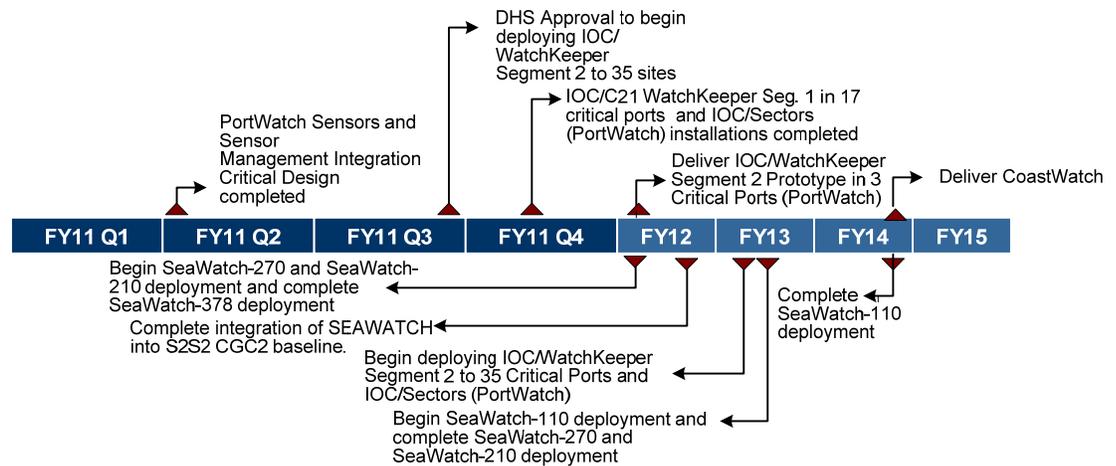
*Long-term Milestones (Years 2-5)*  
FY12: Complete alignment with CG-LIMS (pending CG-9334 programmatic progress/success)

*Critical Success Factors*  
None Identified.

2.2.6 Enhanced Mission C4IT Capability (EMC2)

EMC2 is a C4IT initiative that leverages and uses the expertise of C3CEN, TISCOM and OSC to provide a command and control system for use throughout the Coast Guard and across multiple platforms. This includes strategic operations at the headquarters, area and district level; tactical operations at the sector level; and afloat and airborne operations. Current major strategies include: PortWatch, CoastWatch and SeaWatch. For PortWatch, the Coast Guard will design, build and field a scalable sector-level tactical command and control system with integrated sensors, display, analysis and sharing capabilities that can be tailored to specific port requirements. The target date for PortWatch is 2011. For CoastWatch, the Coast Guard will establish C3CEN as the C2 integrator and developer for strategic enhanced mission command and control across all deepwater and in-service command centers. The target date for CoastWatch is 2012. For SeaWatch, the Coast Guard will design, build and field a transformational modernization initiative that provides mission essential capabilities for Coast Guard Maritime Patrol Aircraft (MPA) and major cutters to include all deepwater and in-service assets. The target date for SeaWatch is 2012. (Primary POC: C4IT Service Center/C3CEN)





**Current Year Milestones**

- FY11 Q2: Complete critical design for PortWatch Sensors and Sensor Management Integration.
- FY11 Q4: Complete installation of IOC/WatchKeeper Segment 1 in 17 Critical Ports and IOCs/Sectors (PortWatch).
- FY11 Q3: Begin SeaWatch-378 deployment and SeaWatch-270, SeaWatch-210 and SeaWatch-110 development

**Long-term Milestones (Years 2-5)**

- FY12: Deliver IOC/WatchKeeper Segment 2 Prototype in 3 Critical Ports (PortWatch)
- FY12: Begin SeaWatch-270 and SeaWatch-210 deployment and complete SeaWatch-378 deployment
- FY12: Complete integration of SEAWATCH into S2S2 CGC2 baseline.
- FY13: Begin deploying IOC/WatchKeeper Segment 2 to 35 Critical Ports and IOC/Sectors (PortWatch)
- FY13: Begin SeaWatch-110 deployment and complete SeaWatch-270 and SeaWatch-210 deployment
- FY14: Deliver CoastWatch
- FY14: Complete SeaWatch-110 deployment
- FY16: Complete IOC/WatchKeeper Segment 2 Deployment at 35 IOCs/Sectors

**Critical Success Factors**

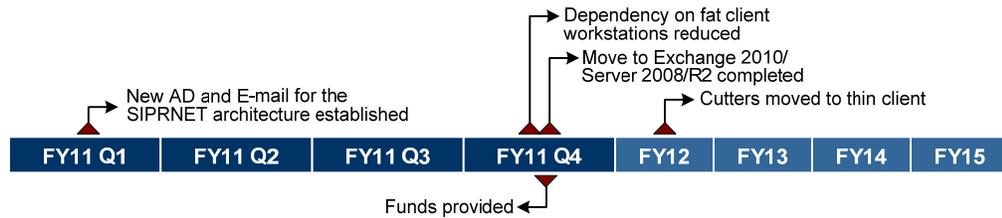
- FY13 Q3: DHS Approval to begin deploying IOC/WatchKeeper Segment 2 to 35 sites

**2.2.7 Information Systems Infrastructure Engineering**

Engineer the enterprise level IT infrastructure necessary to deliver state of the art directory services, e-mail, IT security, collaboration tools, PKI, server and desktop hardware and images in both the SBU and CLASS (SIPRNET) environment. One of the goals is to bring the operating system of SIPRNET servers in line with that of the



SBU network. (Primary POC: C4IT Service Center/TISCOM; Enterprise Information Systems Infrastructure Product Line (EISI-PL))



*Current Year Milestones*

FY11 Q1: Establish a new Active Directory (AD) and E-mail for the SIPRNET architecture

FY11 Q4: Reduce Coast Guard dependency on fat client workstations

FY11Q4: Move to Exchange 2010/Server 2008/R2

*Long-term Milestones (Years 2-5)*

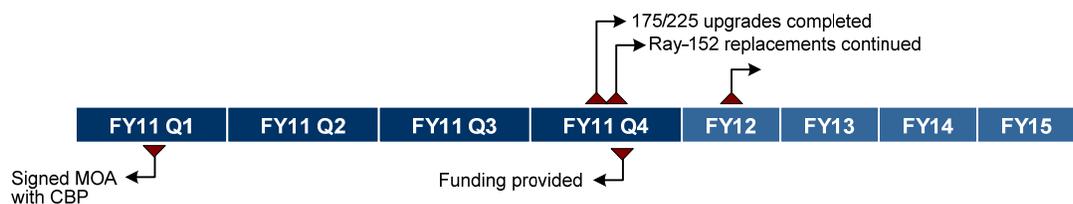
FY12: Transition cutters to thin client

*Critical Success Factors*

FY11 Q4: Funds are provided yearly (the speed of recapitalization is directly related to funds approved)

2.2.8 High Frequency Infrastructure Replacement

Improve high frequency command and control capability by replacing obsolete high power and low power equipment, and implementing High Frequency Automatic Link Establishment (HF ALE). This will be done in synchronization with the COTHEN effort. (POC: C4IT Service Center/C3CEN; Radio Frequency Systems Core Technology (RFS-CT))



*Current Year Milestones*

FY11 Q4: Complete 175/225 upgrades

FY11 Q3: Continue Ray-152 replacements

*Long-term Milestones (Years 2-5)*

FY12: Complete Ray-152 replacements

*Critical Success Factors*

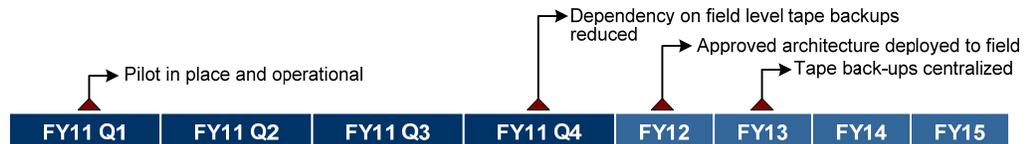
FY11 Q1: Signed MOA with CBP governing interagency agreement on system use

FY12 Q1: AFC-42 funds provided (the speed of deployment is directly related to funds approved)



## 2.2.9 Enterprise Storage and Archiving

Design and implement a solution utilizing the latest backup technologies and best practices and meet the federal security regulations. The solution should ensure data is protected, support remote backup capability over low bandwidth networks, be centrally manageable, reduce media expense, utilize existing acquisition contracts, not impede operational communications, and reduce manual intervention. (POC: C4IT Service Center/TISCOM; Enterprise Information Systems Infrastructure Product Line (EISI-PL))



10132757

### Current Year Milestones

FY11 Q1: Put pilot in place and make operational

FY11 Q4: Reduce dependency on field level tape backups

### Long Term Milestones (Years 2-5)

FY12: Deploy the approved architecture to the field

FY13: Centralize all tape back-ups at OSC for data warehousing

### Critical Success Factors

There are no critical success factors for this initiative.

## 2.2.10 Enterprise Terminal Services

Design and implement a terminal services based workstation access capability using virtual workstations and streaming applications in order to eliminate the need to remotely access desktop work stations. (POC: C4IT Service Center/TISCOM; Enterprise Information Systems Infrastructure Product Line (EISI-PL))



### Current Year Milestones

FY11 Q1: Complete prototype development in lab

FY11 Q3: Deploy field level prototype at prime units

### Long Term Milestones (Years 2-5)

There are no long-term milestones for this initiative.

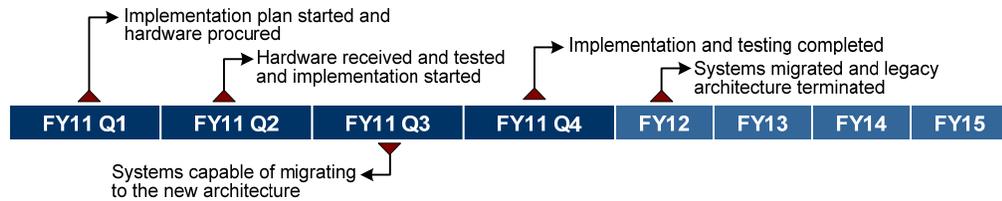
### Critical Success Factors

There are no critical success factors for this initiative.

## 2.2.11 OSC Data Center LAN Upgrade



Upgrade of legacy OSC LAN infrastructure in support of all OSC operations in order meet 99.99 percent availability, Defense Security Technical Implementation Guides, and IPv6 compliance. (POC: C4IT Service Center/OSC)



*Current Year Milestones*

- FY11 Q1: Initiate implementation plan with topology and vendor concurrence and procure hardware
- FY11 Q2: Receive and test all hardware and begin implementation
- FY11 Q3: Continue implementation
- FY11 Q4: Complete implementation and testing

*Long Term Milestones (Years 2-5)*

- FY12: Migrate systems and terminate legacy architecture

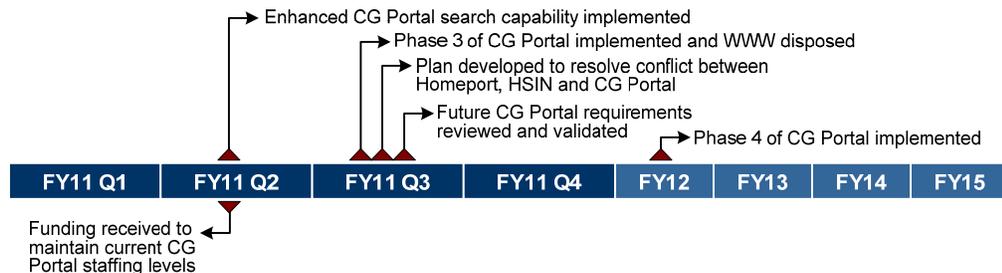
*Critical Success Factors*

- FY11 Q3: Systems capable of migrating to the new architecture when considering other system priorities

## 2.3 Convergence

### 2.3.1 Portal Consolidation

Deliver web-based data and applications via an enterprise Coast Guard Portal (CG Portal) that transcends any particular customer base. This organizational approach to consolidation of multiple portal platforms and disparate web-content delivery mechanisms will provide a single interface for information sharing with active duty and reserve personnel, civilians, auxiliariasts and the public. The CG Portal will serve as the single access point for enterprise content and Coast Guard applications, and a collaborative environment for information sharing between Coast Guard members and external industry partners. (Primary POC: CG-63)



*Current Year Milestones*

- FY11 Q2: Implement enhanced CG Portal search capability



- FY11 Q3: Implement phase 3 of CG Portal and Dispose of WWW
- FY11 Q3: Develop a plan to resolve conflict between Homeport, HSIN and CG Portal
- FY11 Q3: Review and validate future CG Portal requirements and identify improvements to address any gaps

*Long-term Milestones (Years 2-5)*

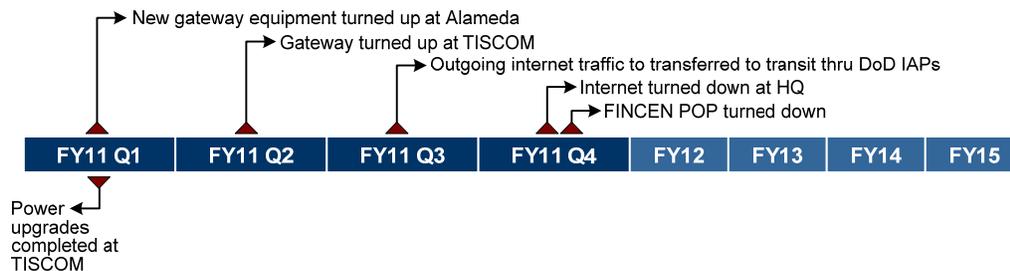
- FY12: Implement Phase 4 of CG Portal

*Critical Success Factors*

- FY11 Q2: Sufficient funding received to maintain current CG Portal staffing levels

2.3.2 Gateway Consolidation and Internet Access

Collapse our current four POPs to 3 Gateways. Direct internet bound traffic to DoD internet access points (IAP) and place all external traffic under advanced DoD monitoring. (Primary POC: C4IT Service Center/TISCOM; Network Infrastructure Product Line (NI-PL))



*Current Year Milestones*

- FY11 Q1: Turn up the new gateway equipment at Alameda
- FY11 Q2: Turn up the gateway at TISCOM
- FY11 Q3: Transfer all outgoing internet traffic to transit thru DoD IAPs
- FY11 Q4: Turn down internet at HQ
- FY11 Q4: Fully turn down FINCEN POP

*Long-term Milestones (Years 2-5)*

There are no long-term milestones for this initiative.

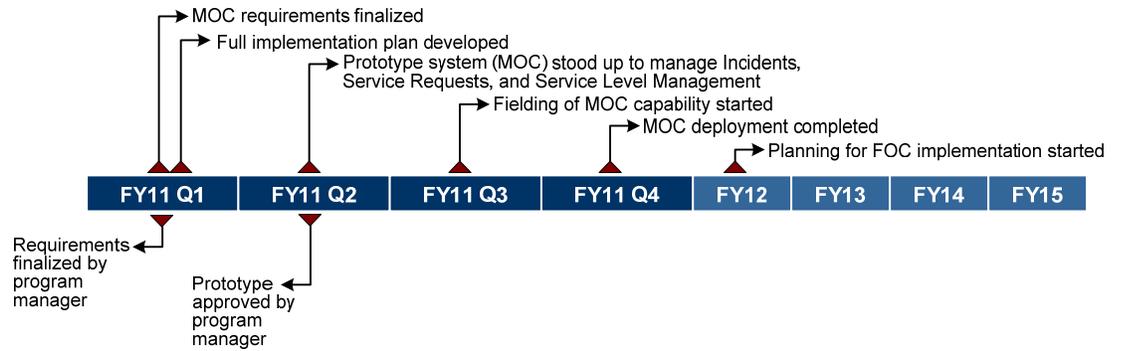
*Critical Success Factors*

- FY11 Q1: Power upgrades must be completed at TISCOM

2.3.3 CGHelp Modernization

The Coast Guard's C4IT Service Center expects to adopt Information Technology Infrastructure Library (ITIL) best practices and standardize and upgrade its service desk software tool suite in concert with its planned update to the next version of BMC Remedy. (Primary POC: C4IT Service Center/OSC)





*Current Year Milestones*

- FY11 Q1: Finalize MOC requirements
- FY11 Q1: Develop full implementation plan
- FY11 Q2: Stand up a prototype system (MOC) to manage Incidents, Service Requests, and Service Level Management
- FY11 Q3: Begin fielding MOC capability to all C4IT support units Coast Guard-wide
- FY11 Q4: Complete implementation of MOC deployment

*Long-term Milestones (Years 2-5)*

- FY12: Begin planning for FOC implementation including implementation of Problems, Knowledge, Configuration Management Data Base, Change, Release, Asset, Service Catalog, Dashboards, and Business Analytics

*Critical Success Factors*

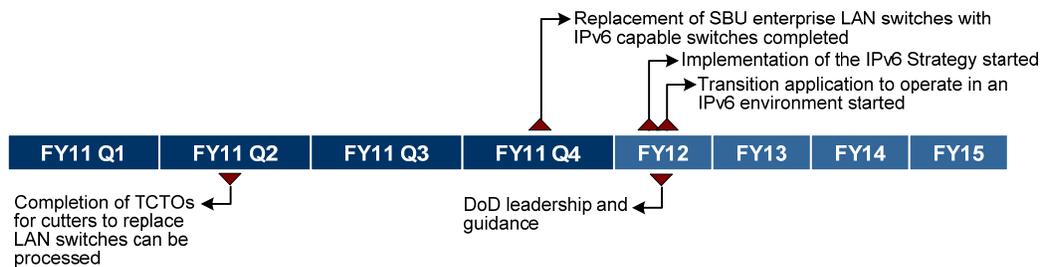
- FY11 Q1: Finalization of requirements by program manager
- FY12 Q2: Prototype approval by program manager

2.4 Net-Centric



## 2.4.1 Coast Guard OneNet Internet Protocol Version 6 (IPv6) Migration

Develop a strategy, architecture, technical implementation plan and support plan to migrate Coast Guard to IPv6. In addition to the upgrade of the Wide Area Network (WAN) and Local Area Network (LAN) hardware to IPv6 capable devices, this incorporates internet protocol de-confliction with DHS OneNet, and coordination with application developers regarding out-year upgrades to IPv6 capable software. (Primary POC: C4IT Service Center/TISCOM; Network Infrastructure Product Line (NI-PL))



### Current Year Milestones

FY11 Q4: Complete replacement of SBU enterprise LAN switches with IPv6 capable switches

### Long-term Milestones (Years 2-5)

FY12: Begin the implementation of the IPv6 Strategy

FY12: Begin to transition application to operate in an IPv6 environment

### Critical Success Factors

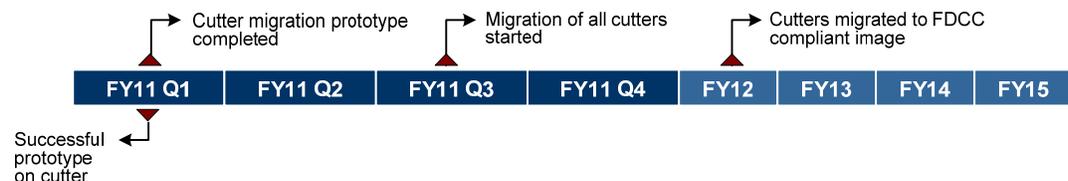
FY11 Q2: Completion of TCTOs for cutters to replace LAN switches can be processed

FY12 Q4: DoD leadership and guidance

## 2.5 Interoperable

### 2.5.1 Common Desktop/ Federal Desktop Core Configuration (FDCC)

Continue to migrate the Coast Guard's standard workstation to the more secure Vista operating system in support of FDCC baseline implementation and deployment as directed by OMB. (Primary POC: C4IT Service Center/TISCOM; Enterprise Information Systems Infrastructure Product Line (EISI-PL))



### Current Year Milestones

FY11 Q1: Complete Cutter migration prototype

FY11 Q3: Begin migration of all cutters



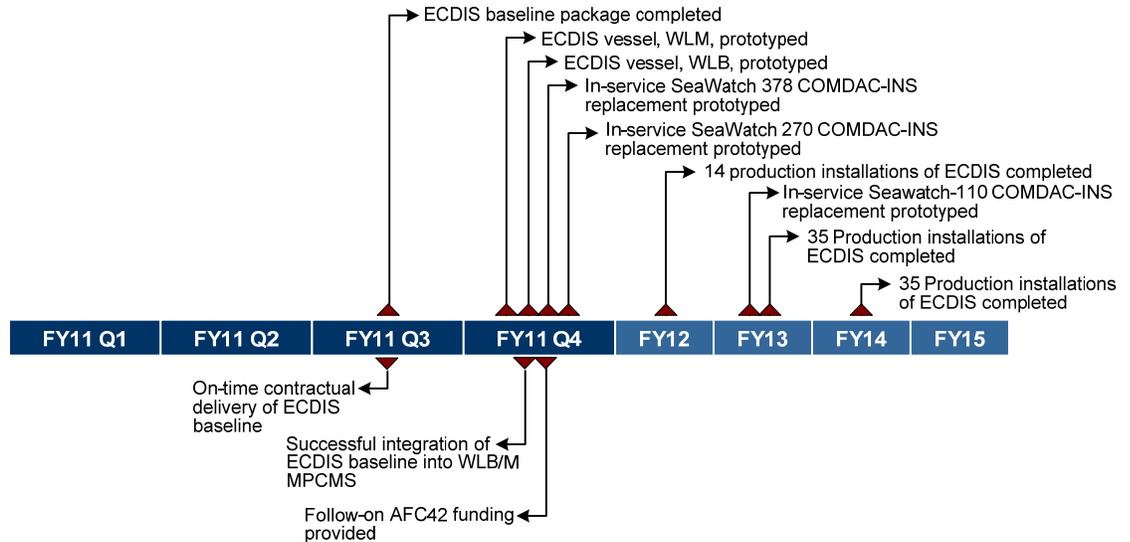
*Long-term Milestones (Years 2-5)*

FY12: Migrate cutters to FDCC compliant image

*Critical Success Factors*

FY11 Q1: Successful prototype on cutter

- 2.5.2 Coast Guard Electronic Chart Display and Information System (CG ECDIS) Development  
As primary development agent for CG-936, develop the CG ECDIS for Sentinel Class patrol boats to be delivered as GFI to Bollinger Shipyards, Inc. (Primary POC: C4IT Service Center/C3CEN).



*Current Year Milestones*

- FY11 Q3: Complete ECDIS baseline package
- FY11 Q4: Prototype an ECDIS vessel, WLM
- FY11 Q4: Prototype an ECDIS vessel, WLB
- FY11 Q4: Prototype an in-service SeaWatch 378 COMDAC-INS replacement
- FY11 Q4: Prototype an in-service SeaWatch 270 COMDAC-INS replacement

*Long-term Milestones (Years 2-5)*

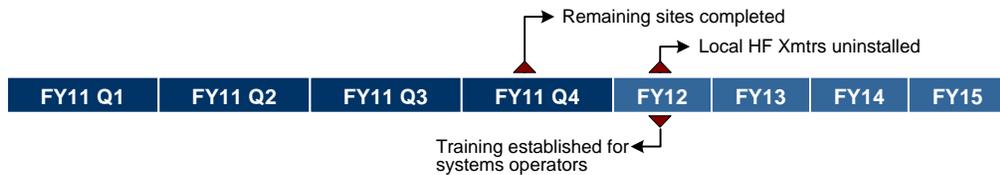
- FY12: Complete 14 production installations of ECDIS
- FY13: Prototype an in-service Seawatch-110 COMDAC-INS replacement
- FY13: Complete 35 production installations of ECDIS
- FY14: Complete 35 Production installations of ECDIS

*Critical Success Factors*

- FY11 Q3: On-time contractual delivery of ECDIS baseline
- FY11 Q4: Successful integration of ECDIS baseline into WLB/M MPCMS
- FY11 Q4: Follow-on AFC42 funding provided



2.5.3 High Frequency Automatic Link Establishment (HF ALE) Network Implementation  
 Improve high frequency command and control capability by developing HF ALE network and enabling sectors and command centers to access and control any HF ALE radio on the network via a Remote Command Console (RCC). (POC: C4IT Service Center/C3CEN; Radio Frequency Systems Core Technology (RFS-CT))



*Current Year Milestones*

FY11 Q4: Complete any remaining/new sites

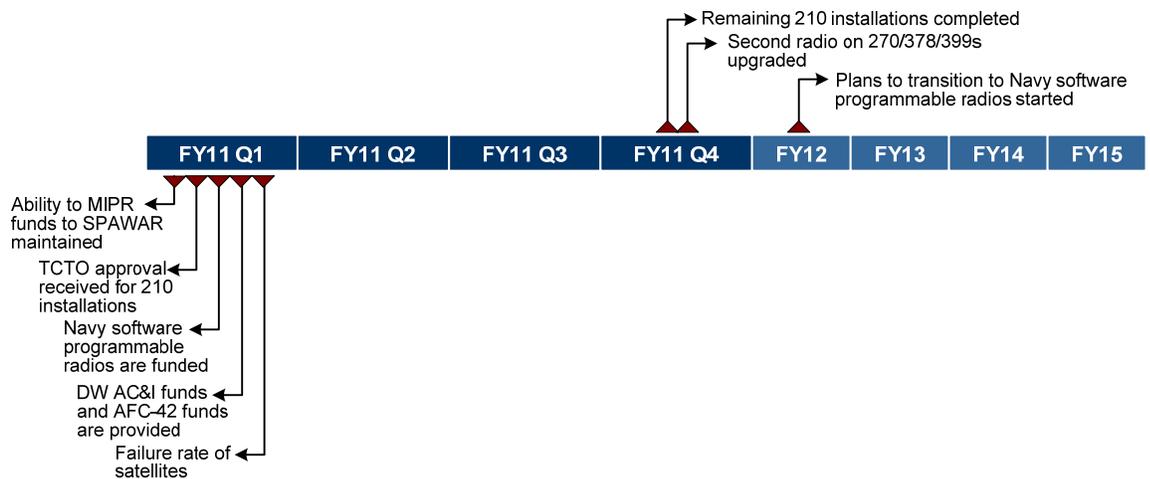
*Long-term Milestones (Years 2-5)*

FY12: Uninstall local HF Xmtrs

*Critical Success Factors*

FY12 Q1: Training established for systems operators

2.5.4 Ultra High Frequency (UHF) Military Satellite Communications (MILSATCOM) Integrated Waveform (IW) Transition  
 Replace and upgrade equipment (on all cutters with UHF MILSATCOM, command centers and mobile units) to enable interoperability with Defense Information Systems Agency (DISA) mandated UHF MILSATCOM waveform. (POC: C4IT Service Center/C3CEN and CG-64; Radio Frequency Systems Core Technology (RFS-CT))



*Current Year Milestones*

FY11 Q4: Complete remaining 210 installations

FY11 Q4: Upgrade second radio on 270/378/399s (funding dependant)



*Long-term Milestones (Years 2-5)*

FY12: Begin plans to transition to Navy software programmable radios (new project)

*Critical Success Factors*

FY11 Q1: Ability to MIPR funds to SPAWAR maintained

FY11 Q1: TCTO approval received for 210 installations

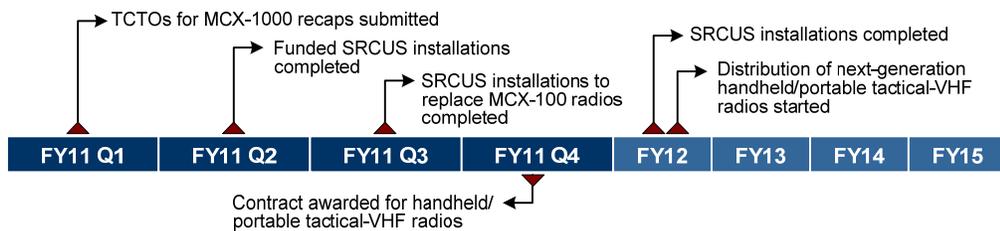
FY11 Q1: Navy software programmable radios are funded

FY11 Q1: DW AC&I funds and AFC-42 funds are provided (the speed of deployment is directly related to funds approved)

FY11 Q1: Availability of legacy (non-IW) channels depends on failure rate of satellites; many are operating past the end of their expected life

2.5.5 Very High Frequency (VHF) Infrastructure

Improve VHF communications capability by implementing a variety of solutions. This includes Short-Range Communications Upgrade System (SRCUS), MCX-1000, VHF trunking, and handheld replacements. This project is linked to the Advanced Encryption Standard (AES) effort. (POC: C4IT Service Center/C3CEN Radio Frequency Systems Core Technology (RFS-CT))



*Current Year Milestones*

FY11 Q1: Submit TCTOs for MCX-1000 recaps (all classes except 378s) to SFLC

FY11 Q2: Complete funded SRCUS installations

FY11 Q3: Complete MCX-1000 recapitalization installations

*Long-term Milestones (Years 2-5)*

FY12: Complete funded SRCUS installations

FY12: Begin distribution of next-generation handheld/portable tactical-VHF radios

*Critical Success Factors*

FY11 Q4: Contract awarded for handheld/portable tactical-VHF radios

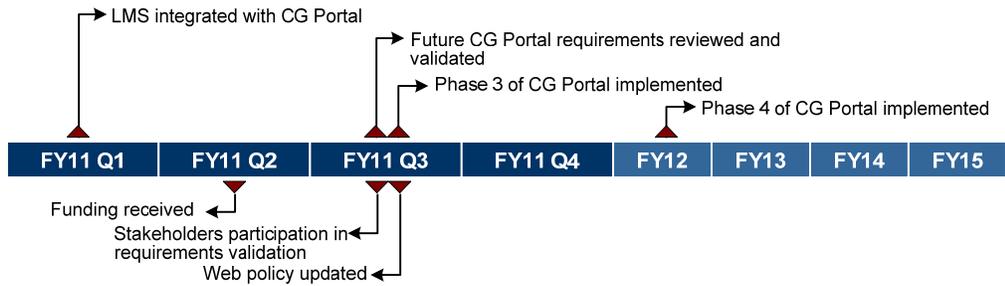
2.6 Innovative

2.6.1 Web 2.0 Strategy

Develop a strategy that defines how the Coast Guard can use Web 2.0 technologies (e.g. social-networking sites, wikis, blogs and podcasts) to improve the Coast Guard's missions and operations; provide transparency to the public and interact with constituents; and enhance information sharing and collaboration within the



Coast Guard and with partners (such as the Navy, Army, Air Force and Border Patrol). (Primary POC: CG-63)



*Current Year Milestones*

- FY11 Q1: Integrate LMS with CG Portal
- FY11 Q3: Review and validate future CG Portal requirements and identify improvements to address any gaps
- FY11 Q3: Implement phase 3 of CG Portal

*Long-term Milestones (Years 2-5)*

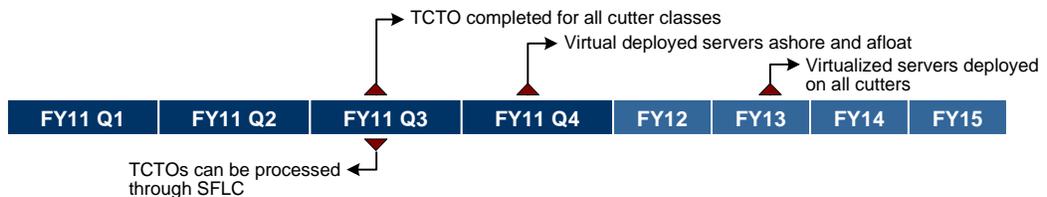
- FY12: Implement phase 4 of CG Portal

*Critical Success Factors*

- FY11 Q2: Sufficient funding received to maintain CG Portal staffing at current levels
- FY11 Q3: Participation by stakeholders in validation of CG Portal requirements identification process
- FY11 Q3: Update of web policy to include social media policies

2.6.2 Server/Workstation Virtualization

Develop a strategy, architecture, technical implementation plan, and support plan to incorporate virtualized servers and workstations into the Coast Guard common operating environment. Server and workstation virtualization will support the goals of promoting green computing, reducing system management resource requirements, and better aligning the physical computing infrastructure to the constrained environments on cutters as well as some shore-based units. (Primary POC: C4IT Service Center/TISCOM; Enterprise Information Systems Infrastructure Product Line (EISI-PL))



*Current Year Milestones*

FY11 Q3: Complete TCTO for all cutter classes

FY11 Q4: Deploy virtual servers ashore and afloat based on funds available and scheduling

*Long-term Milestones (Years 2-5)*

FY13: Complete deployment of virtualized servers on all cutters

*Critical Success Factors*

FY11 Q3: TCTOs can be processed through SFLC



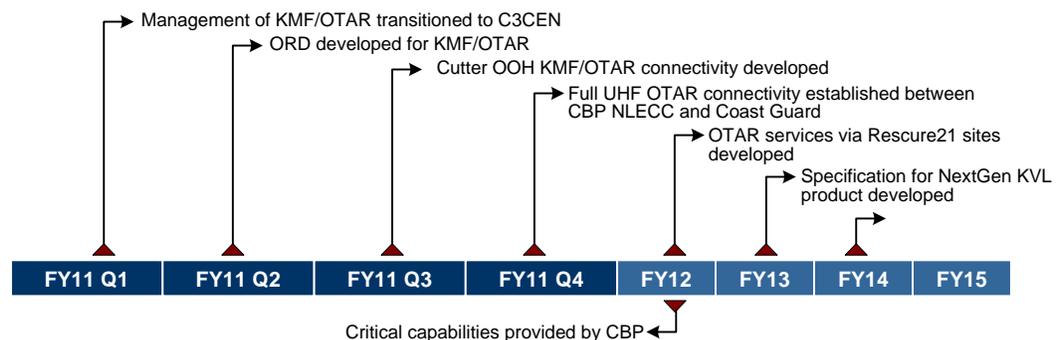
## GOAL 3 SECURITY

### Strategic Activities

#### 3.1 Prevention

##### 3.1.1 Over The Air Rekeying (OTAR)

Implement a centralized Key Management Facility (KMF) for Short Range Communications to affect OTAR throughout the Coast Guard. (Primary POC: CG-64)



##### *Current Year Milestones*

- FY11 Q1: Transition management of KMF/OTAR within the Coast Guard to C3CEN
- FY11 Q2: Develop Organizational Requirements Documents (ORD) for KMF/OTAR
- FY11 Q3: Develop Cutter Out Of Hemisphere (OOH) KMF/OTAR connectivity with CBP NLECC KMC/KMF
- FY11 Q4: Establish full UHF OTAR connectivity between CBP NLECC and Coast Guard

##### *Long-term Milestones (Years 2-5)*

- FY12: Develop OTAR services via Rescue 21 sites (eliminates OTAR regional gaps) (Full Operational Capability (FOC))
- FY13: Develop specification for NextGen KVL product
- FY14: Recap KVL-3000 and replace with NextGen KVL product capable KMF OTAR, Satellite Communication, and Intranet connectivity.

##### *Critical Success Factors*

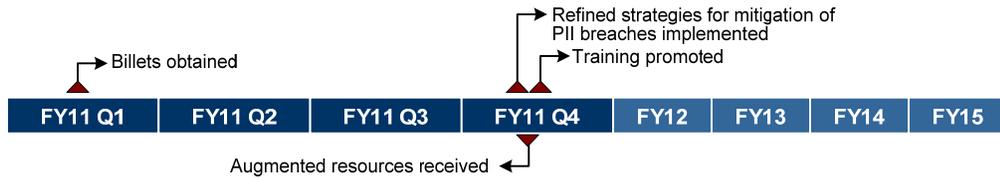
- FY12 Q1: Critical capabilities provided by CBP(enterprises must choose between deploying NLECC and including seamless satellite communication and intranet key encryption deployments)

##### 3.1.2 Personally Identifiable Information (PII) Training

Ensure Coast Guard personnel are trained in safeguarding and handling PII,



including reporting requirements for suspected or actual loss. Identify strategies for mitigation techniques regarding PII. (Primary POC: CG-61)



*Current Year Milestones*

FY11 Q1: Obtain billets and augment program such that mission essential outreach activities/policy development are accomplished in this burgeoning program

FY11 Q4: Implement refined strategies for mitigation of PII breaches

FY11 Q4: Promote training through various means to ensure proper reporting/handling of certain compromised data as incidents occur

*Long-term Milestones (Years 2-5)*

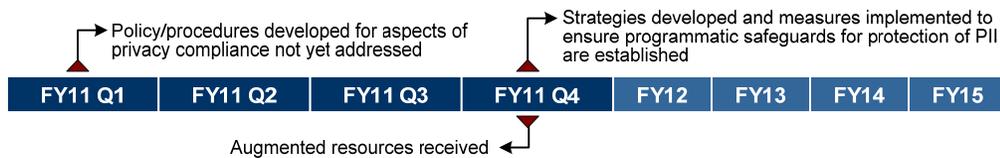
FY12-14: Continue strategic activities discussed for FY11, ensuring additional billets and contractual support are in place to effectively manage the program to meet legal compliance

*Critical Success Factors*

FY11 Q4: Augmented resources

3.1.3 Privacy Compliance/Privacy Threshold Analyses (PTAs)

As a part of managing Personally Identifiable Information (PII) to meet legal requirements, mitigate risks, and conform to provisions of the SDLC, attain Privacy Threshold Analyses (PTAs) for review no later than at the 35 percent systems' design phase. Ensure required compliance documents, including Privacy Impact Assessments (PIAs), System of Record Notices (SORNs), and Notices of Proposed Rulemakings (NPRMs) are consolidated under existing Federal/DHS-wide SORNs or published independently. Update PTAs, PIAs, SORNs and NPRMs for systems significantly changed or amended. (Primary POC: CG-61)



*Current Year Milestones*

FY11 Q1: In addition to meeting DHS, OMB, and SDLC requirements, develop policy/procedures for myriad aspects of privacy compliance not yet published regarding such issues as the collection/use of PII in diverse venues e.g. social media, collaborating with program managers, Public Affairs and Legal



FY11 Q2: Develop strategies and implement measures to ensure programmatic safeguards for protection of PII are established

*Long-term Milestones (Years 2-5)*

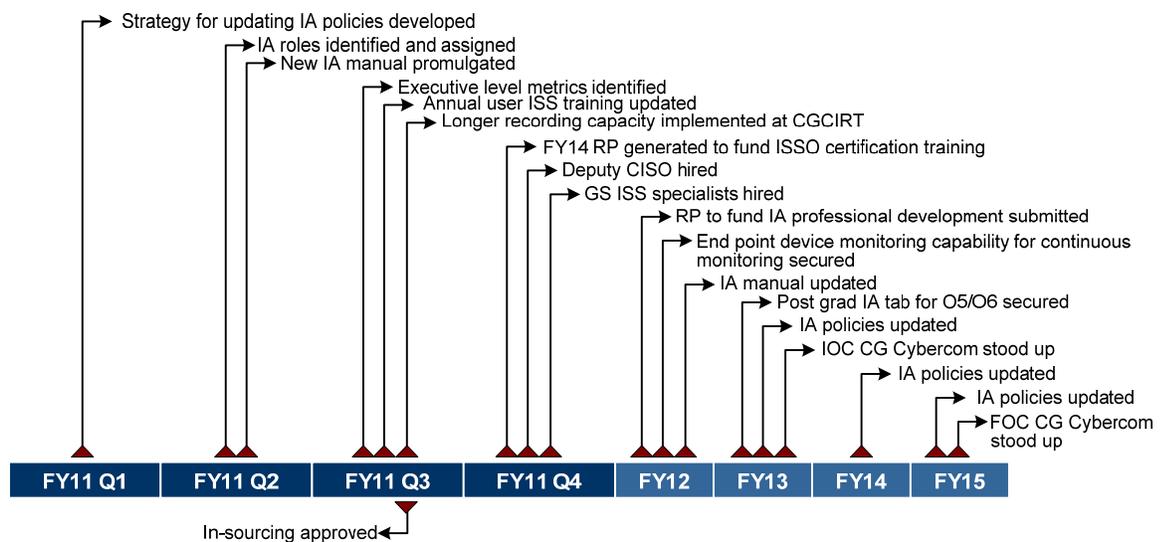
FY12-14: Continue the many activities outlined for FY11 above

*Critical Success Factors*

FY11 Q4: Augmented resources

3.1.4 Strengthening Information Security throughout the Coast Guard

Build the Information Security Program through professional development, policy and key infrastructure investments. Update existing policies. Create policies to address social media, dirty internet connectivity, wireless devices and infosec. (Primary POC: CG-65)



*Current Year Milestones*

FY11 Q1: Develop strategy for updating COMDTINST on SIPRNET management, personal use of government office equipment, non-standard internet connectivity, and wireless device policies

FY11 Q2: Identify IA roles and assign roles to CG-65, C4IT Service Center, TISCOM, and Cybercom Precomdet

FY11 Q2: Promulgate the new IA manual, 5500.13

FY11 Q3: Identify executive level metrics to be integrated in All Flags weekly meeting

FY11 Q3: Update annual user information system security (ISS) training

FY11 Q3: Implement longer recording capacity at CGCIRT

FY11 Q4: Generate FY14 RP to fund ISSO certification training

FY11 Q4: Hire Deputy CISO

FY11 Q4: Hire GS ISS specialists



*Long-term Milestones (Years 2-5)*

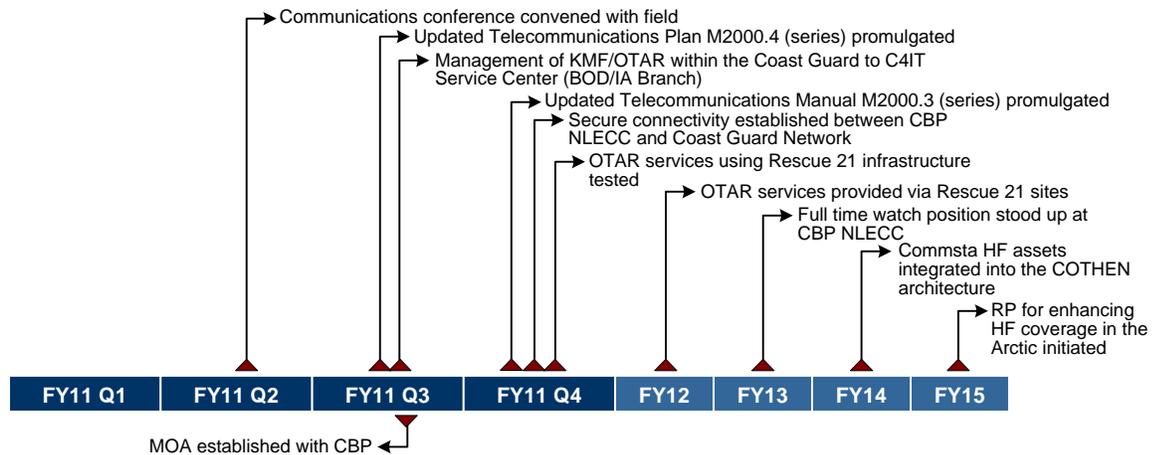
- FY12: Submit RP to fund IA professional development
- FY12: Secure end point device monitoring capability for continuous monitoring
- FY12: Update IA Manual
- FY13: Secure a post grad IA tab for O5/O6
- FY13: Update IA policies
- FY13: Stand up CG Cybercom IOC
- FY14: Update IA policies
- FY15: Update IA policies
- FY15: Stand up CG Cybercom FOC

*Critical Success Factors*

- FY11 Q3: In-sourcing approved

3.1.5 Modernizing the COMMSYS

Implement a centralized Key Management Facility (KMF) for Short Range Communications to affect OTAR throughout the Coast Guard. Expand the COTHEN communications capability for air to ground and command & control for surface assets in addition to air assets. Keep the workforce up to date on latest capabilities, policies and strategic activities. (Primary POC: CG-65)



*Current Year Milestones*

- FY11 Q2: Convene communications conference with field to pass SOP, Policy and training
- FY11 Q3: Promulgate the updated Telecommunications Plan M2000.4 (series)
- FY11 Q3: Transition management of KMF/OTAR within the Coast Guard to C4IT Service Center (BOD/IA Branch)
- FY11 Q4: Promulgate the update to the Telecommunications Manual M2000.3 (series)
- FY11 Q4: Establish secure connectivity between CBP NLECC and Coast Guard Network
- FY11 Q4: Test OTAR services using Rescue 21 infrastructure

*Long-term Milestones (Years 2-5)*

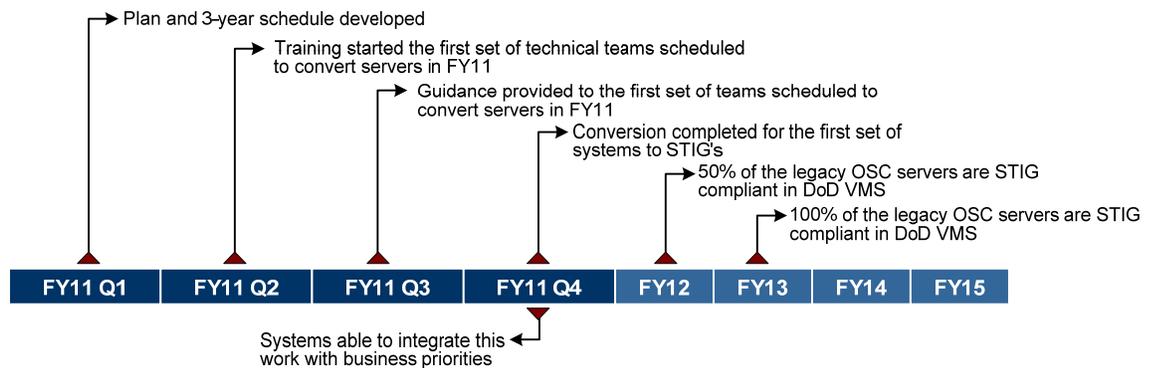
- FY12: Provide OTAR services via Rescue 21 sites (eliminates OTAR regional gaps) (Full Operational Capability (FOC))
- FY13: Stand up a full time watch position at CBP NLECC in Orlando for providing full time voice services to the air and surface fleet
- FY14: Integrate Commsta HF assets into the COTHEN architecture to expand automated coverage
- FY15: Initiate RP for enhancing HF coverage in the Arctic

*Critical Success Factors*

- FY11 Q4: Memorandum of Agreement (MOA) established with CBP

3.1.6 OSC Conversion to DoD Server Hardening Guidelines

In alignment with "Information Assurance Policy - OSC Alignment" memo dated 26 August 2010, OSC will shift from hardening all servers based on DHS Guidelines, to hardening them based on the DoD Security Technical Implementation Guidelines (STIG) over the next three years. (Primary POC: C4IT Service Center/OSC)



*Current Year Milestones*

- FY11 Q1: Develop plan and 3-year schedule
- FY11 Q2: Begin to train the first set of technical teams scheduled to convert servers in FY11
- FY11 Q3: Coordinate and provide guidance to the first set of teams scheduled to convert servers in FY11
- FY11 Q4: Complete conversion of the first set of systems to STIG's

*Long-term Milestones (Years 2-5)*

- FY12: 50 percent of the legacy OSC servers are STIG compliant and are reported in DoD Vulnerability Management System (VMS)
- FY13: 100 percent of the legacy OSC servers are STIG compliant in DoD Vulnerability Management System (VMS)

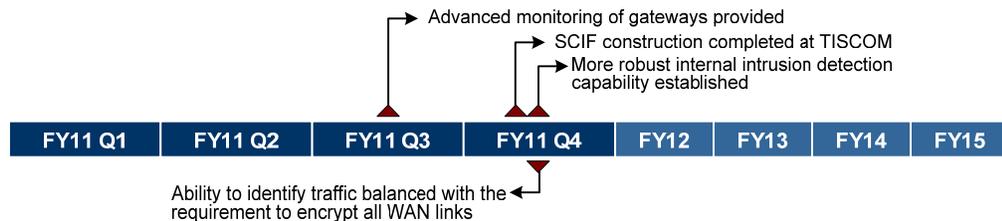
*Critical Success Factors*

- FY11 Q4: Systems are able to integrate this work with business priorities
- Ongoing: Coast Guard security policy continues to track towards DoD focus

### 3.2 Mitigation

#### 3.2.1 Computer Network Defense (CND) Capabilities

Establish CND capabilities that support protecting, monitoring, detecting, analyzing and responding to unauthorized activity and unintentional user errors. (Primary POC: C4IT Service Center/TISCOM)



*Current Year Milestones*

- FY11Q3: Provide advanced monitoring of gateways (in step with 2.3.3)
- FY11 Q4: Complete SCIF construction at TISCOM
- FY11 Q4: Establish a more robust internal intrusion detection capability

*Long-term Milestones (Years 2-5)*

There are no long-term milestones for this initiative.

*Critical Success Factors*

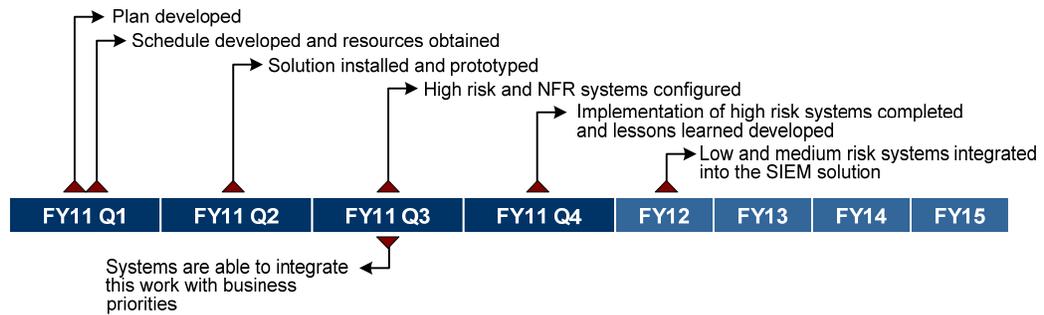
- FY10 Q4: SCIF Design completed in FY10 (funding and prioritization required for construction)



FY11 Q4: Ability to identify traffic balanced with the requirement to encrypt all WAN links

### 3.2.2 Centralized Audit Log

Implementation of a centralized, automated log correlation system in order to address outstanding security requirement identified in numerous system security NFRs and POA&M's. (Primary POC: C4IT Service Center/OSC)



#### *Current Year Milestones*

- FY11 Q1: Develop plan
- FY11 Q1: Develop schedule and obtain resources
- FY11 Q2: Install and prototype solution
- FY11 Q3: Coordinate and configure the high risk and NFR systems
- FY11 Q4: Complete implementation of high risk systems and develop lessons learned

#### *Long-term Milestones (Years 2-5)*

- FY12: Integrate low and medium risk systems into the SIEM solution

#### *Critical Success Factors*

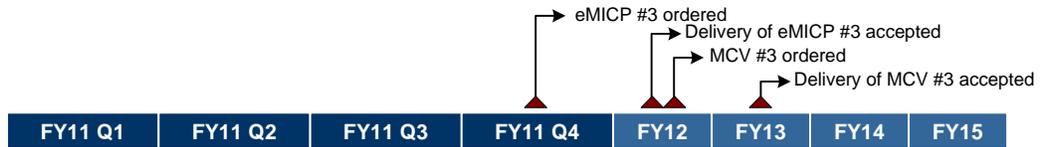
- FY11 Q3: Systems are able to integrate this work with business priorities

## 3.3 Recovery

### 3.3.1 Mobile Command Center (MCC) Development

Improve contingency communications and Continuity of Operations (COOP) capabilities. Develop MCC systems including three enhanced Mobile Incident Command Centers (eMICP) and three Mobile Communications Vans (MCV) to replace the three transportable communication centrals assigned to the Communication Area Master Stations (CAMS). (POC: C4IT Service Center/TISCOM and CG-64)





*Current Year Milestones*

FY11 Q4: Order eMISP #3

*Long-term Milestones (Years 2-5)*

FY12: Accept delivery of eMISP #3

FY12: Order MCV #3

FY13: Accept delivery of MCV #3

*Critical Success Factors*

There are no critical success factors for this initiative.

3.3.2 Contingency SATCOM

Portable system used to restore CG network connectivity in contingency situations. (Primary POC: CG-64) TACHYON system used to establish CG One Net capability via commercial SATCOM path if lost due to natural disaster or some other unexpected event.



*Current Year Milestones*

FY11 Q1: AFC-36 funding received and allocated for FY11 air time costs

*Long-term Milestones (Years 2-5)*

FY12: Consolidate air time costs under KU Band contract (If unsuccessful, continue to request annual air time costs via AFC-36 recurring base)

*Critical Success Factors*

FY12 Q1: Air time plan determined for subsequent fiscal years (either annual recurring or under KU Band air time contract)

3.4 Awareness

See initiative 3.1.4.

3.5 Compliance

See initiative 3.1.4.



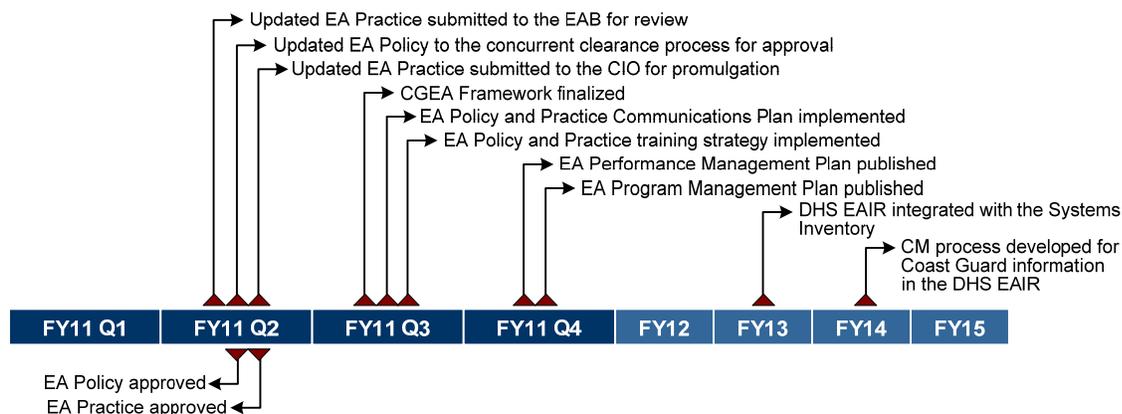
## GOAL 4: GOVERNANCE

### Strategic Activities

#### 4.1 Enterprise Architecture

##### 4.1.1 Coast Guard Enterprise and Segment Architecture

Develop the policies, practices and foundational documents required for the Coast Guard to realize the value of enterprise and segment architecture. Continue to develop, maintain and promote the Coast Guard Enterprise Architecture (CGEA) to enhance decision-making. (Primary POC: CG-66)



##### *Current Year Milestones*

- FY11 Q2: Submit the updated EA Practice to the EAB for review
- FY11 Q2: Submit the updated EA Policy to the concurrent clearance process for approval
- FY11 Q2: Submit the updated EA Practice to the CIO for promulgation
- FY11 Q3: Finalize the CGEA Framework
- FY11 Q3: Implement a Communications Strategy for the new EA Policy and Practice
- FY11 Q3: Implement a training strategy for the new EA Policy and Practice
- FY11 Q4: Publish the EA Performance Management Plan
- FY11 Q4: Publish the EA Program Management Plan

##### *Long-term Milestones (Years 2-5)*

- FY13: Integrate the DHS Enterprise Architecture Information Repository (EAIR) with the Systems Inventory
- FY14: Develop a configuration management (CM) process for Coast Guard information in the DHS EAIR

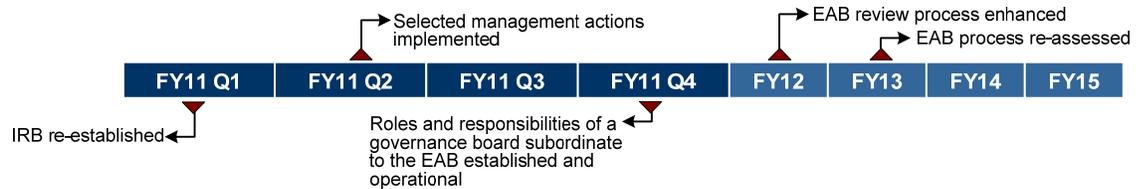
##### *Critical Success Factors*

- FY11 Q2: Approval of the EA Policy



FY11 Q2: Approval of the EA Practice

4.1.2 Coast Guard Enterprise Architecture Board (EAB) and Related EA Reviews  
Align C4IT project investments to the CGEA through technical reviews. (Primary POC: CG-66)



*Current Year Milestones*

FY11 Q2: Implement selected management actions as identified in the C4IT Governance Proof of Concept Exercise

*Long-term Milestones (Years 2-5)*

FY12: Enhance the EAB review process to adhere to DHS requirements and incorporate standard industry practices

FY13: Re-assess the EAB process

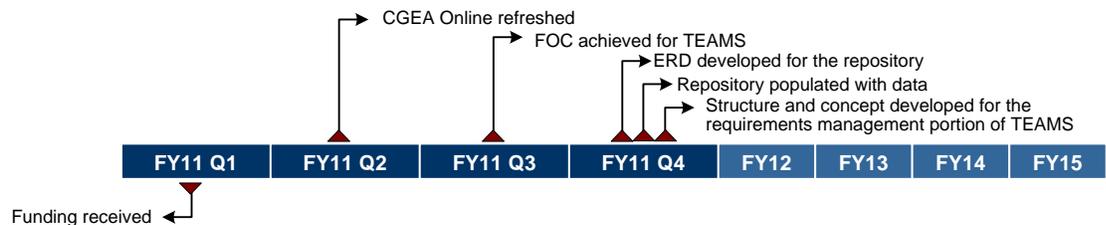
*Critical Success Factors*

FY11 Q1: Re-establishment of the IRB

FY11 Q4: Roles and responsibilities of a governance board subordinate to the EAB established and operational

4.1.3 Enterprise Architecture (EA) Tools

Define and communicate the roles, responsibilities and purpose for existing EA tools (i.e. TEAMS), and develop the related implementation plan. The implementation plan should address resource requirements, initial set-up procedures and parameters, initial and follow-on training pipelines, licensing elements, and periodicity of updates and reports. In addition, the implementation plan should clearly delineate the office of responsibility. (Primary POC: CG-66)



*Current Year Milestones*

FY11 Q2: Refresh CGEA Online

FY11 Q3: Achieve FOC for TEAMS

FY11 Q4: Develop an Entity Relationship Diagram (ERD) for the repository

FY11 Q4: Populate the repository with data



FY11 Q4: Develop structure and concept for the requirements management portion of TEAMS

*Long-term Milestones (Years 2-5)*

No milestones currently scheduled for FY11 through FY15.

*Critical Success Factors*

FY11 Q1: Funding received for contract to develop ERD

4.1.4 Service Oriented Architecture (SOA)

Establish an Integrated Project Team (IPT) to identify Coast Guard requirements for SOA. (Primary POC: CG-66)



*Current Year Milestones*

FY11 Q1: Work with SOA IPT to develop the Mission Needs Statement for SOA

FY11 Q1: Work with the SOA IPT to develop the SOA Concept of Operations (CONOPS)

*Long-term Milestones (Years 2-5)*

No milestones currently scheduled for FY11 through FY15.

*Critical Success Factors*

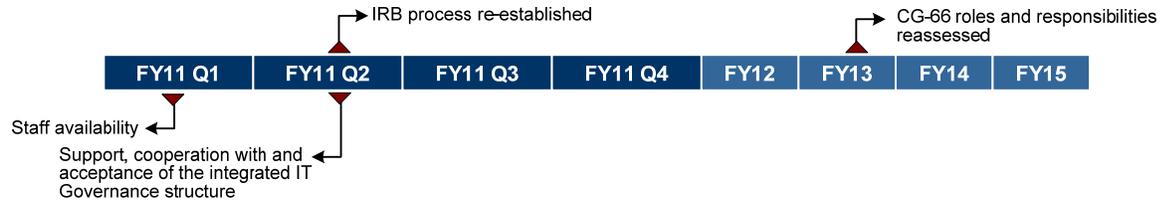
FY11 Q1: Staff availability

## 4.2 Capital Planning and Investment Control

4.2.1 Governance Process Integration

Integrate multiple governance processes (i.e. processes for Coast Guard acquisitions, the DHS EAB, Coast Guard EAB, ITAR, MSAM, SDLC, DHS Management Directive (MD) 102, DHS Systems Engineering Life Cycle (SELC) Acquisition Directive 102-01, and Acquisition Instruction/Guidebook, 102-01-001) into a singular streamlined governance process to select, acquire, use, maintain and dispose of C4IT investments. The process will use best practices for Capital Planning and Investment Control (CPIC) such as the Control Objectives for Information and related Technology (COBIT) framework. (Primary POC: CG-66)





*Current Year Milestones*

FY11 Q2: Re-establish the IRB process to ensure required actions are performed

*Long-term Milestones (Years 2-5)*

FY13: Reassess CG-66 roles and responsibilities in Coast Guard CPIC, ITAR and SDLC processes

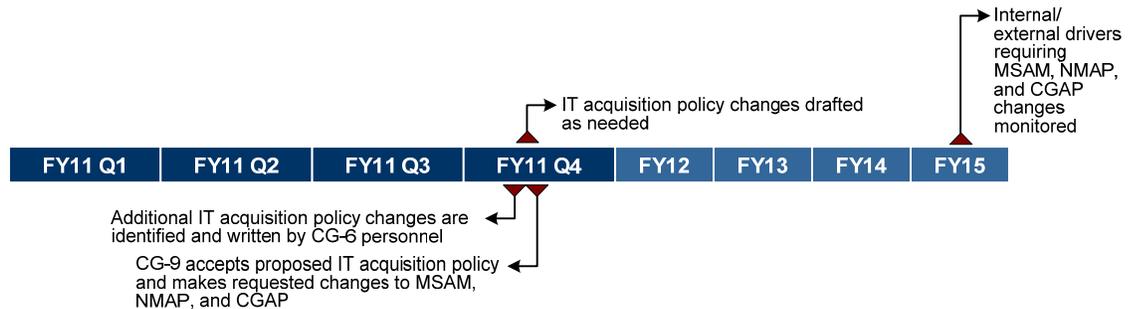
*Critical Success Factors*

FY11 Q1: Staff availability outside of CG-66

FY11 Q2: Support, cooperation with and acceptance of the integrated IT Governance structure

4.2.2 CG-9 Alignment

Work with CG-9 to define roles, responsibilities, policies and practices for C4IT acquisitions. (Primary POC: CG-69)



*Current Year Milestones*

FY11 Q4: Draft IT acquisition policy changes to MSAM, Non-Major Acquisition Procedures (NMAP), and CG Acquisition Procedures (CGAP) as needed

*Long-term Milestones (Years 2-5)*

FY12-15: Monitor internal/external drivers requiring MSAM, NMAP, and CGAP changes

*Critical Success Factors*

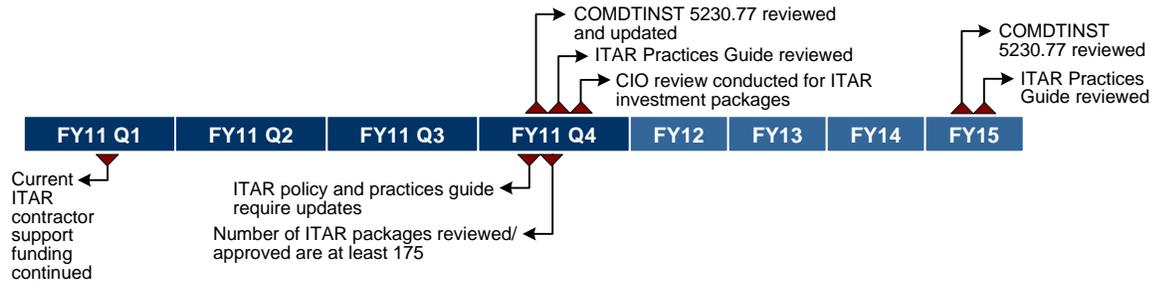
FY11 Q4: Additional IT acquisition policy changes are identified and written by CG-6 personnel

FY11 Q4: CG-9 accepts proposed IT acquisition policy and makes requested changes to MSAM, NMAP, and CGAP

4.2.3 Information Technology Acquisition Review (ITAR) Process



Continue to leverage, institutionalize and refine the ITAR Process. (Primary POC: CG-69)



*Current Year Milestones*

- FY11 Q4: Review and update COMDTINST 5230.77, Implementation of Coast Guard and DHS CIO Review and Approval of C4IT Acquisitions Equal to or Greater than \$2.5M as needed to ensure currency with DHS CIO Management Directives
- FY11 Q4: Review ITAR Practices Guide to ensure currency with DHS CIO Management Directives and review and approval processes (update as necessary)
- FY11 Q4: Conduct CIO review and approval of 175 ITAR investment packages

*Long-term Milestones (Years 2-5)*

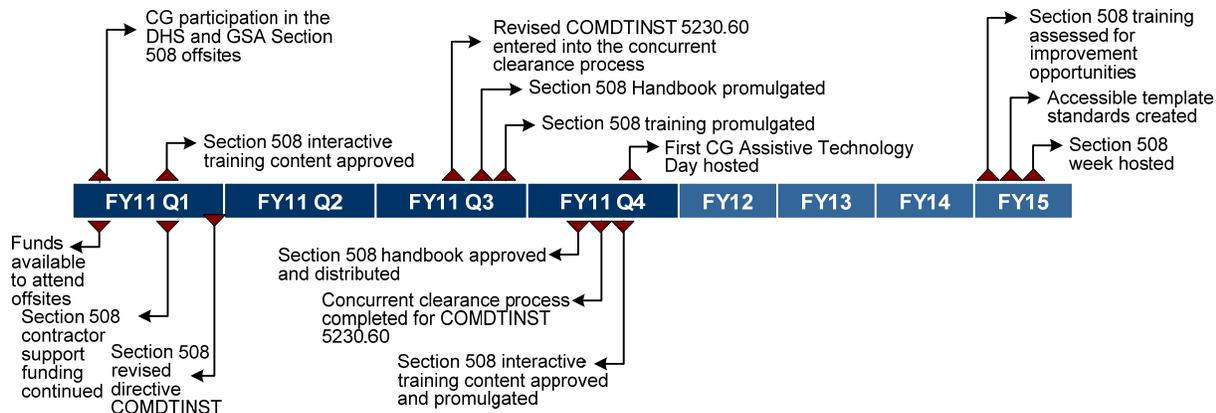
- FY12-15: Review COMDTINST 5230.77, Implementation of Coast Guard and DHS CIO Review and Approval of C4IT Acquisitions Equal to or Greater than \$2.5M to ensure currency with DHS CIO Management Directives (update policy as needed)
- FY12-15: Review ITAR Practices Guide to ensure currency with DHS CCIO management Directives and review and approval processes (update as necessary)

*Critical Success Factors*

- FY11 Q1: Current ITAR contractor support funding is continued
- FY11 Q4: ITAR policy and practices guide require updates
- FY11 Q4: Number of ITAR packages reviewed/approved are at least 175

4.2.4 Section 508 Program Management  
 Institutionalize and refine the Coast Guard Section 508 Program to improve Coast Guard Section 508 awareness and compliance. (Primary POC: CG-69)





### Current Year Milestones

- FY11 Q1: Participate in the DHS Section 508 offsite and GSA Section 508 offsite
- FY11 Q1: Obtain approval for Section 508 interactive training content
- FY11 Q3: Enter the revised CG Directive COMDTINST 5230.60, CG Implementation of the Rehabilitation Act, into the concurrent clearance process
- FY11 Q3: Complete development and promulgate Section 508 training
- FY11 Q3: Promulgate the Section 508 Handbook
- FY11 Q4: Host the first CG Assistive Technology Day

### Long-term Milestones (Years 2-5)

- FY12 -15: Assess Section 508 Training for opportunities for improvement, Implement Training enhancements derived from FY12 training assessment
- FY12 -15: Create accessible template standards for Coast Guard documents
- FY12 -15: Host Coast Guard Section 508 week

### Critical Success Factors

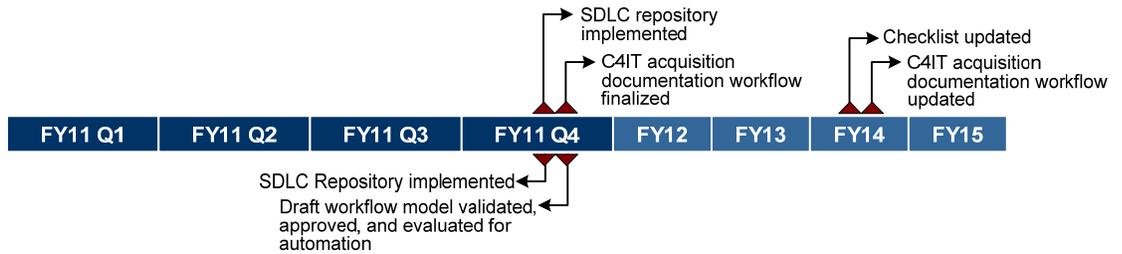
- FY11 Q1: Funds are available to attend the DHS Section 508 offsite and GSA Section 508
- FY11 Q1: Section 508 revised directive COMDTINST
- FY11 Q1: Section 508 contractor support funding continued
- FY11 Q4: Section 508 Handbook approved and distributed
- FY11 Q4: Concurrent clearance process completed for COMDTINST 5230.60
- FY11 Q4: Section 508 interactive training content approved and promulgated

#### 4.2.5 Acquisition Processes Communication and Workflow

Create a customer-centric checklist that provides a single list of necessary end-to-end compliance activities. This checklist should leverage the significant progress CG-6 has made in mapping processes across SDLC, ITAR and MSAM. While providing integration, the checklist should not require the customer to decipher



between separate processes. In the long term, the Coast Guard will also consider implementing an automated workflow and document repository to facilitate the storage and retrieval of C4IT acquisition documents. (Primary POC: CG-69)



*Current Year Milestones*

- FY11 Q4: Implement SDLC Repository
- FY11 Q4: Finalize C4IT acquisition documentation workflow

*Long-term Milestones (Years 2-5)*

- FY11-14: Update checklist
- FY12-14: Update C4IT acquisition documentation workflow

*Critical Success Factors*

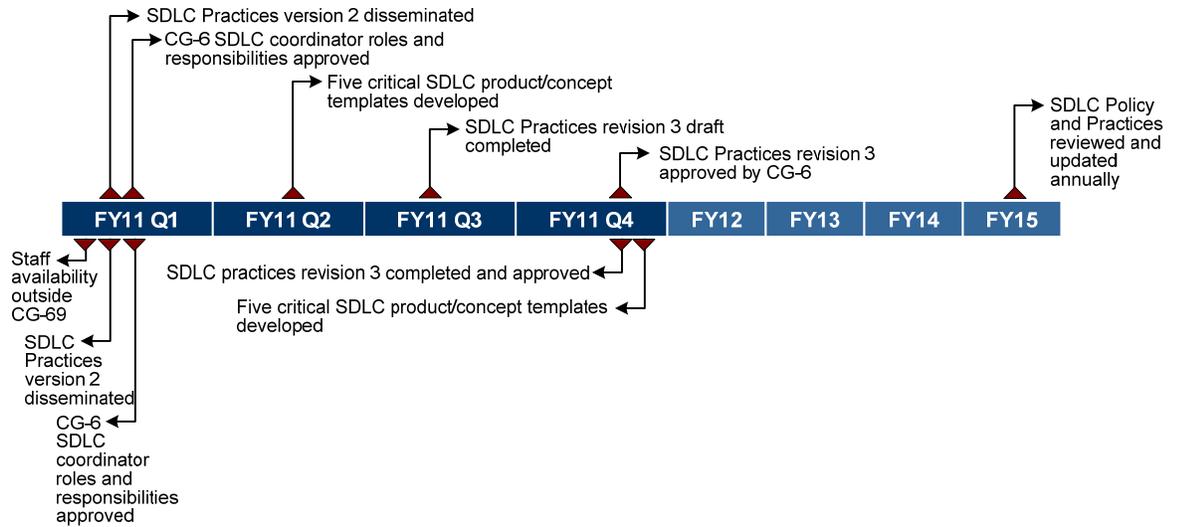
- FY11 Q4: SDLC Repository implemented
- FY11 Q4: Draft workflow model validated, approved, and evaluated for automation; automation opportunities are identified

### 4.3 Systems Development Life Cycle

#### 4.3.1 Manage the Systems Development Life Cycle (SDLC) Policy

Update the SDLC Policy to reflect the current state of SDLC implementation at the Coast Guard. The SDLC Policy establishes the authority, roles, and responsibilities for the governance of the Coast Guard’s System Development Life Cycle (SDLC) for Command, Control, Communications, Computers, and Information Technology (C4IT) systems. The SDLC provides a consistent process for C4IT project management, including designated phases and decision points. This policy governs all C4IT systems developed and managed by the Commandant (CG-6), Sponsors, System Development Agents (SDAs), and System Support Agents (SSAs). It applies to all C4IT assets, including systems and products that enable C4IT capability in support of the Coast Guard’s missions or business functions. (Primary POC: CG-69)





**Current Year Milestones**

- FY11 Q1: Disseminate SDLC Practices version 2 throughout CG
- FY11 Q1: Obtain CG-6 approval of the CG-6 SDLC coordinator roles and responsibilities.
- FY11 Q2: Develop five critical SDLC product/concept templates (requires assistance from CG-66 and CG-64)
- FY11 Q3: Complete draft of SDLC Practices revision 3
- FY11 Q4: SDLC Practices revision 3 approved by CG-6

**Long-term Milestones (Years 2-5)**

- FY12-15: SDLC Policy and Practices are reviewed annually and updated as needed and additional SDLC product/concepts templates are developed as needed

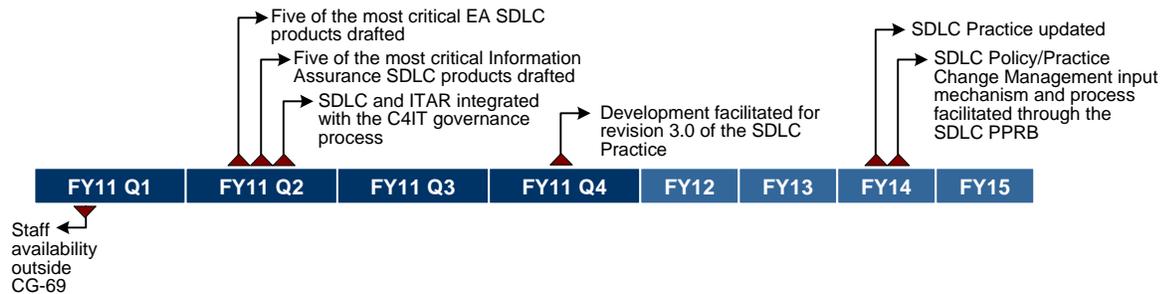
**Critical Success Factors**

- FY11 Q1: Staff availability outside CG-69 (particularly CG-66 and CG-64 with SDLC EA and IA templates)
- FY11 Q1: SDLC Practices version 2 disseminated throughout the CG
- FY11 Q1: CG-6 SDLC coordinator roles and responsibilities approved
- FY11 Q4: Draft of SDLC practices revision 3 completed and approved
- FY11 Q4: Five critical SDLC product/concept templates developed



#### 4.3.2 Manage the Systems Development Life Cycle (SDLC) Practice

Update the SDLC Practice to reflect the current state of SDLC implementation at the Coast Guard. The SDLC Practice provides detailed instructions for adherence to the SDLC processes throughout the life cycle of a system. It applies to all C4IT assets, including systems and products that enable C4IT capability in support of the Coast Guard's missions or business functions. (Primary POC: CG-69)



##### *Current Year Milestones*

- FY11 Q2: Partner with CG-66 to draft five of the most critical EA SDLC products
- FY11 Q2: Partner with CG-64 to draft five of the most critical Information Assurance SDLC products
- FY11 Q2: As a C4IT Governance WG member, work with CG-66 to integrate SDLC and ITAR with the C4IT governance process
- FY11 Q4: Facilitate the development of a draft SDLC Practice revision 3.0

##### *Long-term Milestones (Years 2-5)*

- FY 12-14: Update the SDLC Practice
- FY12-14: Facilitate the SDLC Policy/Practice Change Management input mechanism and process thru SDLC PPRB

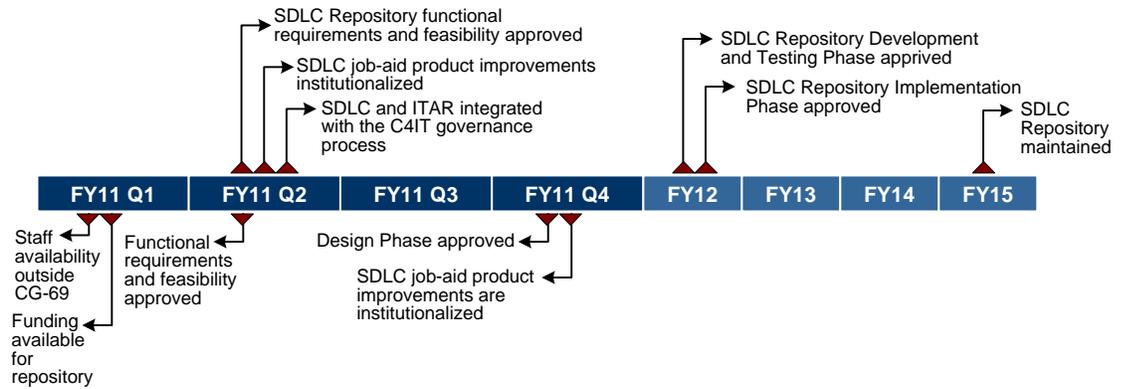
##### *Critical Success Factors*

- FY11 Q1: Staff availability outside CG-69 (particularly CG-66 and CG-64 with SDLC EA and IA templates)

#### 4.3.3 Manage the Systems Development Life Cycle (SDLC) Repository

Develop and manage an SDLC repository for SDLC job-aid products, such as templates, guides and checklists. The SDLC Repository will support SDLC Policy and Practice implementation throughout the Coast Guard by providing a single, authoritative source for the storage and retrieval of all C4IT acquisition documents that is easily accessible and available enterprise-wide. (Primary POC: CG-69)





**Current Year Milestones**

**FY11 Q2:** Functional requirements and feasibility for the SDLC Repository Concept approved and approval is provided to enter SDLC Design Phase Approval

**FY11 Q2:** Institutionalize SDLC job-aid product improvements

**Long-term Milestones (Years 2-5)**

**FY12:** Obtain SDLC Repository Development and Testing Phase Approval

**FY12:** Obtain SDLC Repository Implementation Phase Approval

**FY13-15:** Maintain the SDLC Repository

**Critical Success Factors**

**FY11 Q1:** Staff is available outside CG-69 to assist with the development of SDLC repository functional requirements

**FY11 Q1:** Funding is available for repository development

**FY11 Q2:** Functional requirements and feasibility for SDLC Repository Concept is approved and repository entered into the SDLC

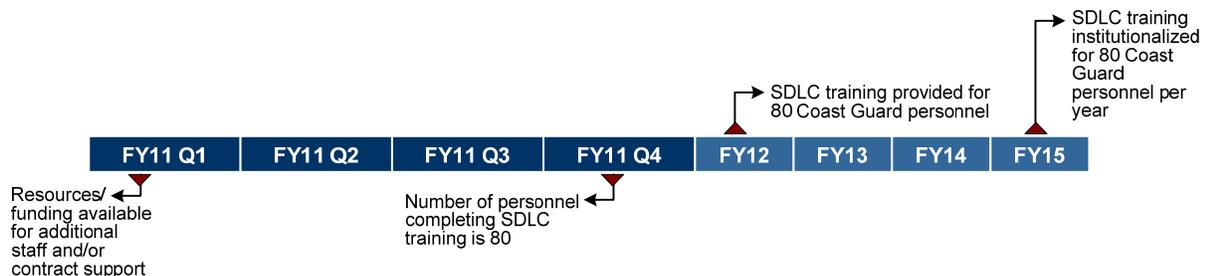
**FY11 Q4:** Design Phase approval

**FY11 Q4:** SDLC job-aid product improvements are institutionalized

**4.3.4 Manage the Systems Development Life Cycle (SDLC) Training**

Provide training to Coast Guard personnel on the Coast Guard’s SDLC process.

The SDLC training will support SDLC policy and practice implementation throughout the Coast Guard. (Primary POC: CG-69)



*Current Year Milestones*

FY11 Q4: Provide SDLC training for 80 Coast Guard personnel

*Long-term Milestones (Years 2-5)*

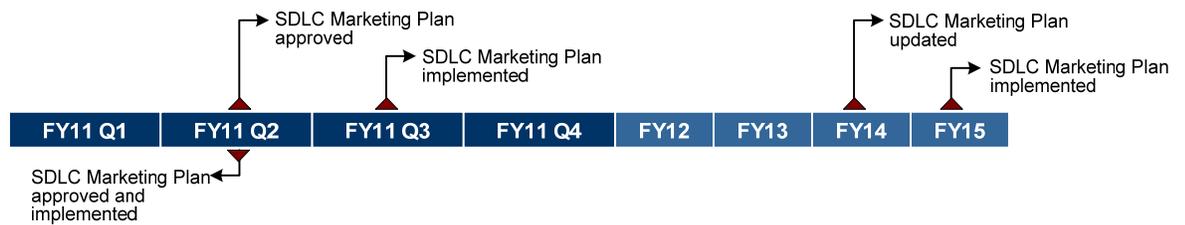
FY12-15: Institutionalize/Conduct SDLC training for 80 Coast Guard personnel per year

*Critical Success Factors*

FY11 Q1: Resources/funding available for additional staff and/or contract support

FY11 Q4: Number of personnel completing SDLC training is 80

- 4.3.5 Manage Systems Development Life Cycle (SDLC) Communications and Outreach  
Manage the communication, outreach and indoctrination of the SDLC process to help promote and institutionalize the SDLC. SDLC communication and outreach will support SDLC Policy and Practice implementation throughout the Coast Guard. (Primary POC: CG-69)



*Current Year Milestones*

FY11 Q2: CG-6 approves the SDLC Marketing Plan

FY11 Q3: Implement the SDLC Marketing Plan

*Long-term Milestones (Years 2-5)*

FY12 -14: Update the SDLC Marketing Plan

FY12-15: Implement the SDLC Marketing Plan

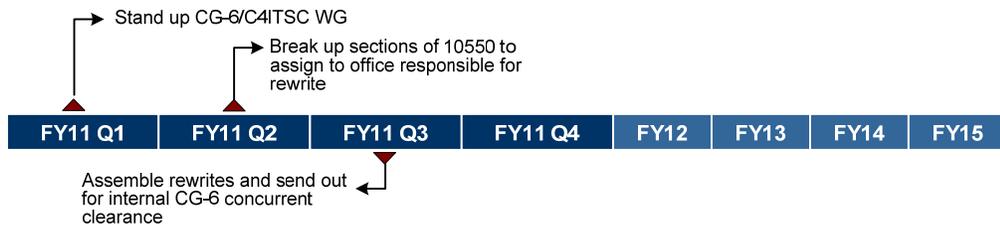
FY12-15: Update the SDLC Marketing Plan as necessary

*Critical Success Factors*

FY11 Q2: SDLC Marketing Plan is approved and implemented

- 4.3.6 COMDTINST M10550, Electronics Manual, Update  
CIM 10550 promulgates Coast Guard electronic life cycle policy and selected procedures. This includes guidance on procuring, installing, maintaining, and managing supported electronic equipment within the Coast Guard. This Manual also provides guidance for safety information and professional development for the Coast Guard's Electronics Technician. The purpose of this initiative is to update the manual to reflect the most current electronic life cycle procedures. (Primary POC: CG-64)





*Current Year Milestones*

FY11 Q1: Stand up CG-6/C4ITSC WG

FY11 Q2: Break up sections of 10550 to assign to office responsible for rewrite

FY11Q4: Assemble rewrites and send out for internal CG-6 concurrent clearance

*Long-term Milestones (Years 2-5)*

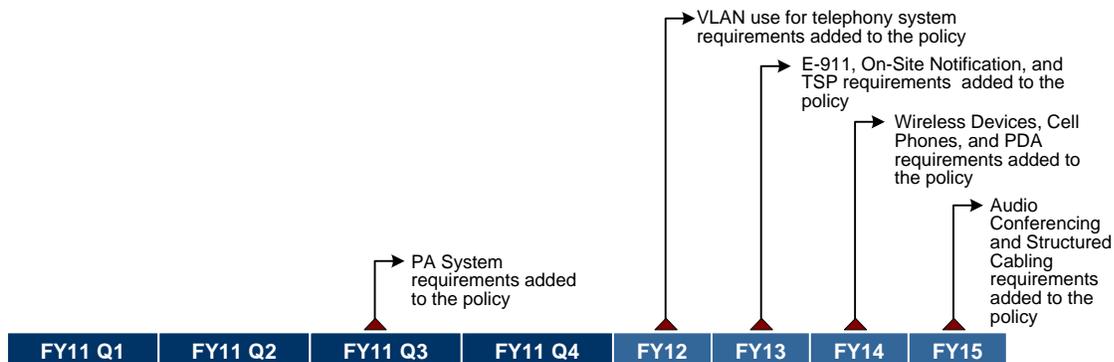
None identified.

*Critical Success Factors*

None identified.

4.3.7 Telephony Systems Policy

Develop policy for telephony systems. (Primary POC: CG-64)



*Current Year Milestones*

FY11 Q3: Add Public Address (PA) System requirements to the policy document

*Long-term Milestones (Years 2-5)*

FY12: Add VLAN use for telephony system requirements to the policy document

FY13: Add E-911, On-Site Notification, and TSP requirements to the policy document

FY14: Add Wireless Devices, Cell Phones, and PDA requirements to the policy document



FY15: Add Audio Conferencing and Structured Cabling requirements to the policy document

*Critical Success Factors*

Ongoing: Participation of all CG-6/C4ITSC-TISCOM Offices and the TVD+V Working Group members

#### 4.4 Performance Measurement

There are no strategic activities in this area for FY11.

#### 4.5 Project Management

There are no strategic activities in this area for FY11.

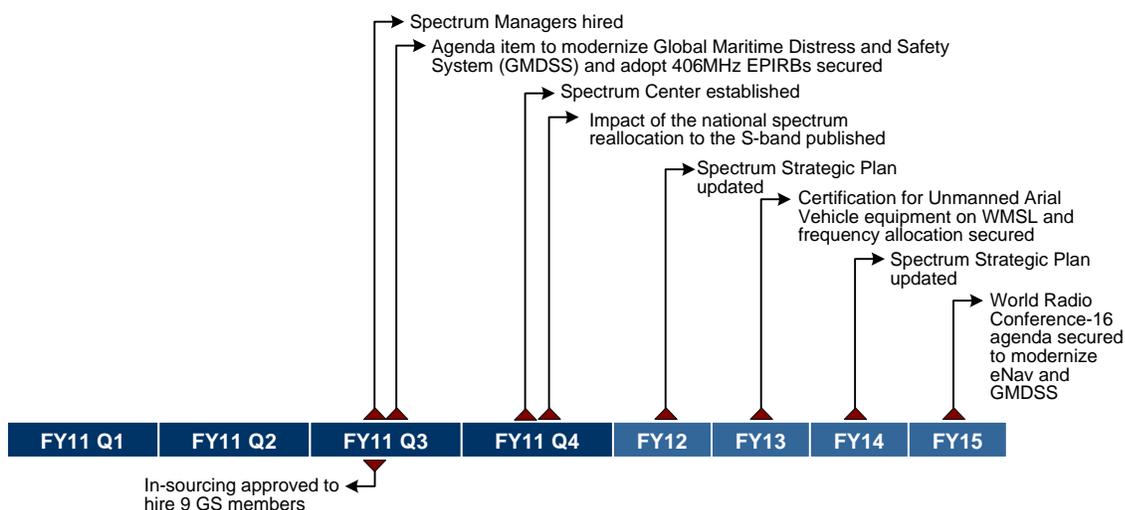
#### 4.6 Requirements

There are no strategic activities in this area for FY11.

#### 4.7 Standards

##### 4.7.1 Strengthen Spectrum Program to Ensure Mission Success

Support the development of policies and tools that use electromagnetic spectrum effectively in support of Coast Guard operations. Proactively engage international forums on the electromagnetic spectrum to advocate for global policies that benefit future Coast Guard capabilities. (Primary POC: CG-65)



*Current Year Milestones*

FY11 Q3: Hire spectrum managers as part of the in-sourcing effort

FY11 Q3: Secure agenda item to modernize Global Maritime Distress and Safety System (GMDSS) and adopt 406MHz EPIRBs during next IMO Convention



FY11 Q4: Establish Spectrum Center

FY11 Q4: Publish the impact of the national spectrum reallocation to the S-band on Coast Guard and public mariners

*Long-term Milestones (Years 2-5)*

FY12: Update the Spectrum Strategic Plan

FY13: Secure certification for Unmanned Aerial Vehicle equipment on WMSL and secure frequency allocation

FY14: Update the Spectrum Strategic Plan

FY15: Secure World Radio Conference-16 agenda to modernize eNav and GMDSS

*Critical Success Factors*

FY11 Q3: In-sourcing approved to hire nine GS members



## GOAL 5: ORGANIZATIONAL EXCELLENCE

### Strategic Activities

#### 5.1 Customer Service

##### 5.1.1 Center of Excellence (COE) Standardization

Support the Coast Guard's transformation by consolidating the centers of excellence into an integrated C4IT Service Center that will provide full life-cycle management and bi-level maintenance support for Coast Guard people, platforms and systems. (Primary POC: C4IT Service Center/Business Operations Division (BOD))

*Current Year Milestones*  
None identified.

*Long-term Milestones (Years 2-5)*  
None identified.

*Critical Success Factors*  
None identified.

##### 5.1.2 Industry Best Practices Adoption and Execution

Continue to leverage best practices (i.e. Information Technology Infrastructure Library (ITIL), Capability Maturity Model Integration (CMMi), and Lean Six Sigma) to ensure the delivery of high-quality customer service. (Primary POC: C4IT Service Center/BOD)

*Current Year Milestones*  
None identified.

*Long-term Milestones (Years 2-5)*  
None identified.

*Critical Success Factors*  
None identified.

#### 5.2 Workforce Development

##### 5.2.1 C4IT Professional Development

Provide guidance to help develop our personnel and allow for success as a Coast Guard C4IT professional. This includes the creation of Individual Development Plans (IDPs) to help employees develop their skills, achieve their career goals and further the mission of CG-6. (Primary POC: CG-6D/CG-6EA)

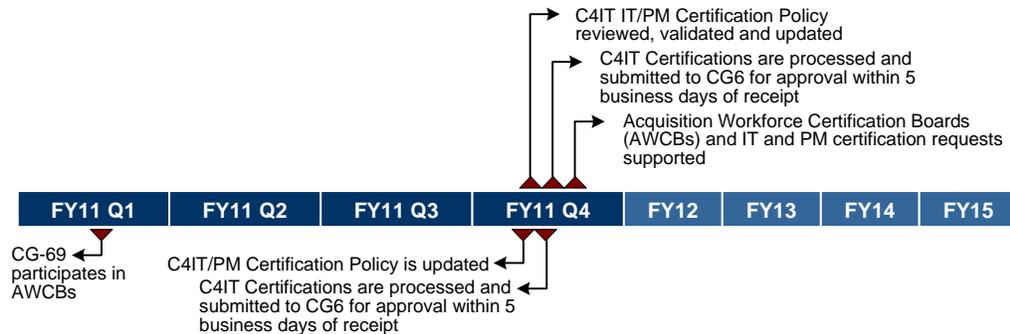
*Current Year Milestones*  
None identified.



*Long-term Milestones (Years 2-5)*  
None identified.

*Critical Success Factors*  
None identified.

- 5.2.2 IT/Program Manager Certification Policy  
Establish the CG-6 Policy for Information Technology and Program Manager Certifications for all C4IT personnel (civilian and military). (Primary POC: CG-69)



*Current Year Milestones*

- FY11 Q4: Review and validate C4IT IT/PM Certification Policy and update as necessary
- FY11 Q4: Process and submit C4IT Certifications to CG-6 for approval within 5 business days of receipt
- FY11 Q4: Participate in Acquisition Workforce Certification Boards (AWCBs) and support IT and PM certification requests

*Long-term Milestones (Years 2-5)*

- FY12-15: Continue to participate in AWCBs
- FY12-15: Review and validate C4IT IT/PM Certification Policy and update as necessary
- FY12-15: Continue to process C4IT IT/PM Certifications

*Critical Success Factors*

- FY11 Q1: CG-69 participates in Acquisition Workforce Certification Boards
- FY11 Q4: C4IT/PM Certification Policy is updated, if necessary
- FY11 Q4: C4IT Certifications are processed and submitted to CG6 for approval within 5 business days of receipt

5.3 Process Improvement

- 5.3.1 St. Elizabeth Requirements  
Identify and develop infrastructure requirements for St. Elizabeths. (Primary POC: CG-64)



*Current Year Milestones*

None identified.

*Long-term Milestones (Years 2-5)*

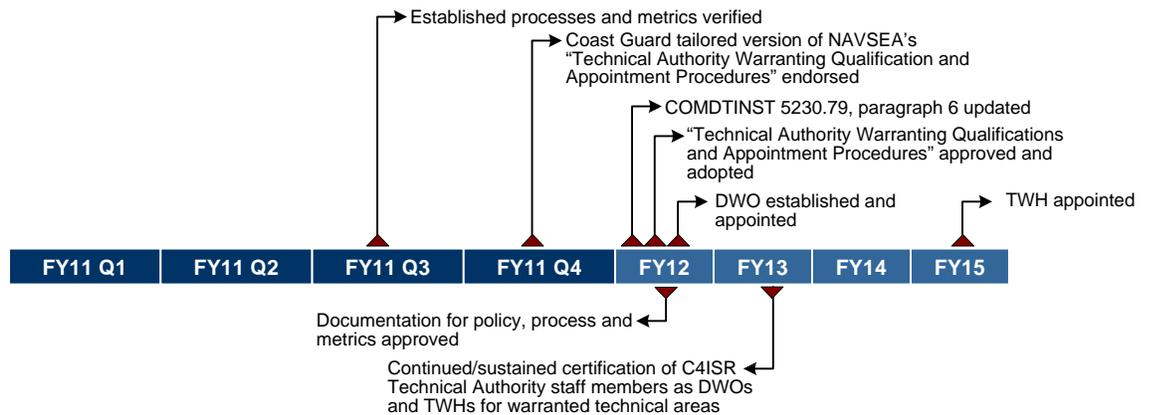
None identified.

*Critical Success Factors*

None identified.

5.3.2 Establishment of CG-6 Technical Authority

Establish documented technical authority processes and metrics for the design, development, deployment, security, and maintenance of all Coast Guard C4IT systems. This includes those enterprise-wide C4IT systems and sub-systems that support aviation, research and development, and deepwater missions. The guidelines will provide information about technical authority roles and responsibilities, processes, and certifications. (Primary POC: CG-6 and the C4IT Service Center)



*Current Year Milestones*

FY11 Q3: Verify established processes and metrics

FY11 Q4: Endorse a Coast Guard tailored version of NAVSEA's "Technical Authority Warranting Qualification and Appointment Procedures"

*Long-term Milestones (Years 2-5)*

FY12: Update COMDTINST 5230.79, paragraph 6

FY12: Obtain approval and support adoption of the Coast Guard tailored "Technical Authority Warranting Qualifications and Appointment Procedures"

FY12: Establish and appoint a Deputy Warranting Officer (DWO) in accordance with the "Technical Authority Warranting Qualifications and Appointment Procedures"

FY15: Appoint the Technical Warrant Holder (TWH) in accordance with "Technical Authority Warranting Qualifications and Appointment Procedures" for a warranted technical area



*Critical Success Factors*

FY12: Approved documentation for policy, process and metrics

FY13: Continued/sustained certification of C4ISR Technical Authority staff members as DWOs and TWHs for warranted technical areas

5.3.3 Configuration Management Alignment of NTNO and NTCGO Systems

Align SCIF NTNO and NTCGO with looking at configuration control with the Navy future roadmap. Align Navy CM problems for the NAVSSI/GPNTS, TACAN/JPAL and Moriah. (Primary POC: CG-64)

*Current Year Milestones*

None identified.

*Long-term Milestones (Years 2-5)*

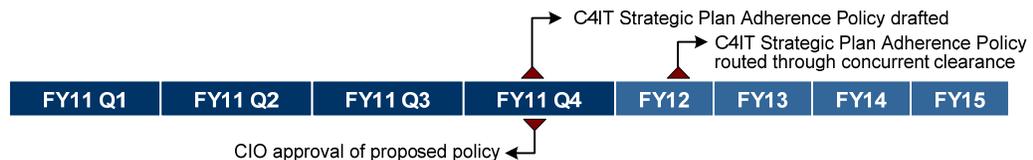
None identified.

*Critical Success Factors*

None identified.

5.3.4 C4IT Strategic Plan Adherence

Draft and enact a COMDTINST that requires adherence to the C4IT Strategic Plan for C4IT operations, projects and priorities. This COMDTINST will require units and offices working on C4IT to align their plans with goals and objectives identified in the C4IT Strategic Plan. In addition, it will establish the process, roles and responsibilities for maintaining the C4IT Strategic Plan and monitoring adherence to the plan's goals, objectives and strategic activities. (Primary POC: CG-66)



*Current Year Milestones*

FY11 Q4: Draft a policy to enforce adherence to the C4IT Strategic Plan and submit to CIO for approval before concurrent clearance

*Long-term Milestones (Years 2-5)*

FY12: Route the C4IT Strategic Plan Adherence Policy through the concurrent clearance process

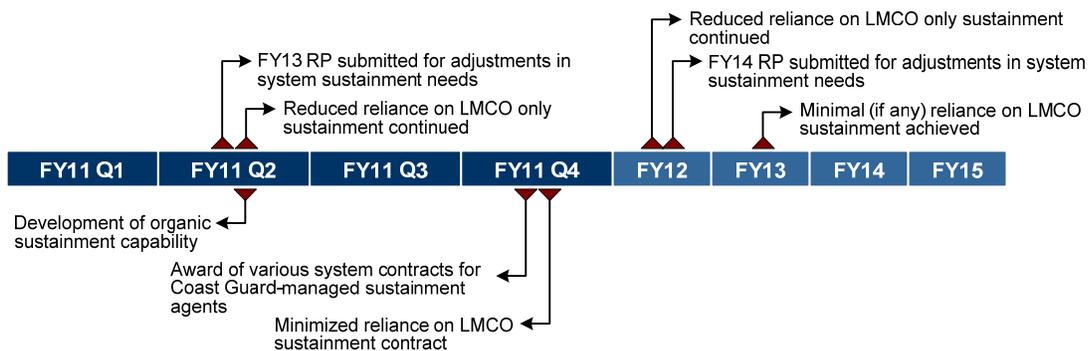
*Critical Success Factors*

FY11 Q4: CIO approval of proposed policy

5.3.5 Transition to Efficient Sustainment of Deepwater Command, Control, Communications, Combat, Computing, Intelligence, Surveillance, and Reconnaissance (C5ISR) Systems  
Continue the transition of sustainment for Command, Control, Communications, Combat, Computing, Intelligence, Surveillance, and Reconnaissance (C5ISR) systems acquired through and currently supported by Integrated Coast Guard Systems, Limited Liability Corporation (ICGS, LLC) and Lockheed-Martin



Corporation's Maritime Systems & Sensors (LMCO MS2) Division. The Integrated Deepwater Systems (IDS) model included life-cycle support by ICGS, LLC for all C5ISR assets. Due to the reliability issues associated with complexity and extensive use of LMCO MS2 proprietary software, sustainment costs for the limited number of Coast Guard acquired IDS systems has become increasingly unaffordable. This initiative continues the transition of sustainment from ICGS, LLC to a sole-source contract with LMCO MS2 (Phase 1); identifying competitive support opportunities for Commercial Off The Shelf (COTS) components (e.g. TRS-3D Radar) (Phase 2); and eventual recapitalization of CG-C2 and other Special Not Off The Shelf (SNOTS) proprietary systems with reliable, interoperable and sustainable Government/Commercial Off The Shelf (GOTS/COTS) solutions (Phase 3). (Primary POC: C4IT Service Center/BOD; Business Operations Divisions Technical Authority Branch (BOD-TAB))



**Current Year Milestones**

- FY11 Q1: Submit FY13 RP for adjustments in system sustainment needs
- FY11 Q2: Complete C4IT Service Center (COEs) identification of a schedule (a POAM for specific systems) for transitioning to Coast Guard managed sustainment (i.e. organic and Coast Guard-managed contracts)
- FY11 Q2: Continue to reduce reliance on LMCO only sustainment

**Long-term Milestones (Years 2-5)**

- FY12: Continue to reduce reliance on LMCO only sustainment
- FY12: Submit FY14 RP for adjustments in system sustainment needs
- FY13: Achieve minimal (if any) reliance on LMCO sustainment

**Critical Success Factors**

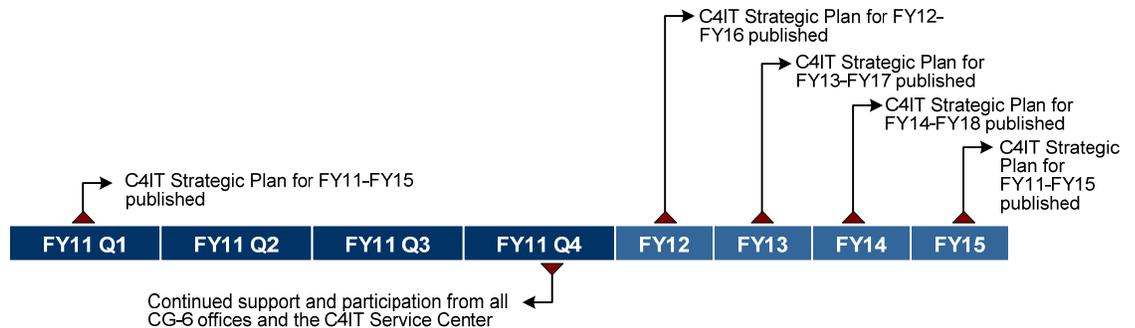
- FY11Q2: Development of organic sustainment capability
- FY11 Q4: Award of various system contracts for Coast Guard-managed sustainment agents, where organic sustainment is not appropriate
- FY11 Q4: Minimized reliance on LMCO sustainment contract

**5.4 Outreach**



#### 5.4.1 Communication of the CG-6 Strategy and Related Strategic Activities

Develop and implement communications tactics to ensure that we share information about the Coast Guard's C4IT strategy and strategic activities with internal and external stakeholders. (Primary POC: CG-6)



##### *Current Year Milestones*

FY11 Q1: Publish the C4IT Strategic Plan for FY11-FY15

##### *Long-term Milestones (Years 2-5)*

FY12: Publish the C4IT Strategic Plan for FY12-FY16

FY13: Publish the C4IT Strategic Plan for FY13-FY17

FY14: Publish the C4IT Strategic Plan for FY14-FY18

FY15: Publish the C4IT Strategic Plan for FY15-FY19

##### *Critical Success Factors*

FY11 Q1: Continued support and participation from all CG-6 offices and the C4IT Service Center

#### 5.4.2 C4IT and Engineering Outreach Events

Conduct outreach events to provide open opportunities for members of our specialties and ratings to ask career questions, identify deficiencies in organizational performance, and provide information on new strategic activities, training, and education opportunities. (Primary POC: CG-6)

##### *Current Year Milestones*

None identified.

##### *Long-term Milestones (Years 2-5)*

None identified.

##### *Critical Success Factors*

None identified.

### 5.5 Performance Measurement

There are no strategic activities in this area for FY11.



# APPENDIX B: STRATEGIC ALIGNMENT MATRICES

## ALIGNMENT OF THE COMMANDANT'S GUIDING PRINCIPLES AND C4IT GOALS

USCG C4IT GOALS DHS CIO GOALS	Information	Technology	Security	Governance	Organizational Excellence
Steady the service				✓	✓
Honor our profession					✓
Strengthen our partnerships	✓			✓	✓
Respect our shipmates					✓

Source: ALCOAST 271/10



## ALIGNMENT OF DHS IT GOALS AND COAST GUARD C4IT GOALS

USCG C4IT GOALS DHS CIO GOALS	Information	Technology	Security	Governance	Organizational Excellence
Goal 1: Establish secure IT services and capabilities to protect the Homeland and enhance our Nation's preparedness, mitigation and recovery capabilities.		✓	✓		
Goal 2: Strengthen and unify the Department's ability to share information and services internally and with Federal, State, local, tribal, international and private industry partners.	✓	✓			
Goal 3: Improve transparency, accountability, and efficiencies of services and programs through effective governance.				✓	
Goal 4: Develop and implement a comprehensive approach to IT employee recruitment, development, retention and recognition to ensure excellence in IT delivery across the Department.					✓

Source: DHS Information Technology Strategic Plan Fiscal Years 2011-2015



## ALIGNMENT OF COAST GUARD STRATEGIC PRIORITIES FOR FY10 AND C4IT GOALS

USCG C4IT GOALS	Information	Technology	Security	Governance	Organizational Excellence
USCG STRATEGIC PRIORITIES FOR FY10					
Recapitalize Operating Assets and Sustain Infrastructure		✓		✓	
Enhance Maritime Safety and Security	✓	✓	✓	✓	✓
Modernize Business Practices		✓	✓		✓
Optimize Workforce Capacity					✓

Source: U.S. Coast Guard Posture Statement (2009)



## ALIGNMENT OF THE COAST GUARD STRATEGY FOR SAFETY, SECURITY AND STEWARDSHIP AND C4IT GOALS

USCG C4IT GOALS	Information	Technology	Security	Governance	Organizational Excellence
USCG STRATEGY FOR SAFETY, SECURITY & STEWARDSHIP					
Strengthen regimes for the U.S. maritime domain			✓	✓	
Achieve awareness in the Maritime Domain	✓	✓	✓	✓	
Enhance unity of effort in maritime planning and operations	✓	✓	✓	✓	✓
Integrate Coast Guard capabilities for national defense	✓	✓	✓	✓	
Develop a national capacity for Marine Transportation System recovery	✓	✓	✓	✓	
Focus international engagement on improving maritime governance	✓	✓	✓	✓	

Source: U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship (2007)



## ALIGNMENT OF THE CG-DCMS BUSINESS PLAN AND COAST GUARD C4IT GOALS

USCG C4IT GOALS CG-DCMS OBJECTIVES	Information	Technology	Security	Governance	Organizational Excellence
Execute APO stand-up, pilots and product line transformation					
Transition MLCs / ISCs functions to DCMS					
Stand-up five DCMS Logistics Centers / Service Centers					✓
Achieve USCG Business Model FY09 logistics transformation objectives					
Attain mission support performance goals				✓	
Plan and execute the human capital strategy (FY09)					✓
Fund and execute CFO compliant DCMS transformations					
Implement senior executive outreach communication campaign					
Demonstrate CG-LIMS development and implementation		✓			
Oversee and manage non-major acquisitions and Coast Guard systems integrator					✓
Execute acquisition reform				✓	
Implement disciplined mission support governance				✓	

Source: DCMS Fiscal Year 2009 Modernization Business Plan (2008)



## ALIGNMENT OF DHS IT INFRASTRUCTURE INITIATIVES AND COAST GUARD C4IT INITIATIVES

USCG C4IT GOALS DHS INITIATIVES	Information	Technology	Security	Governance	Organizational Excellence
Network Services Consolidation		✓			
Data Center Consolidation		✓			
E-mail Services		✓			
Single Sign-On			✓		
Wireless Services		✓			
Communications Security			✓		
Cybersecurity			✓		

Source: The State of DHS IT Infrastructure, July 2008 – December 2008 (2008)



## ALIGNMENT OF THE DOD INFORMATION SHARING STRATEGY AND COAST GUARD C4IT GOALS

USCG C4IT GOALS	Information	Technology	Security	Governance	Organizational Excellence
DoD INFORMATION SHARING STRATEGY					
Promote, encourage, and create incentives for sharing	✓	✓	✓	✓	✓
Achieve an extended enterprise	✓	✓	✓	✓	
Strengthen agility, in order to accommodate unanticipated partners and events	✓	✓	✓	✓	✓
Ensure trust across organizations	✓	✓	✓	✓	

Source: DoD Information Sharing Strategy (2007)



## APPENDIX C: ACRONYMS

AAP(s)	Advanced Acquisition Plan(s)	CAO	Chief Acquisition Officer
ADEX	Active Directory Exchange	CAS	Core Accounting System
AES	Advanced Encryption Standard	CDRP	Contingency and Disaster Recovery Plan
AIS	Automatic Identification System	CFO	Chief Financial Officer
ALD	Aviation Logistics Division	CG	Coast Guard
ALS	Automated LORAN System	CG-DCMS	Coast Guard's Deputy Commandant of Mission Support
AMHS	Automated Message Handling System	CG ECINS	Coast Guard Electronic Charting Integrated Navigation System
AMVER	Automated Mutual-assistance Vessel Rescue system	CG OneNet	Coast Guard OneNet
APO	Asset Project Office	CG Portal	Coast Guard Portal
AOA	Analysis of Alternatives	CG-LIMS	Coast Guard Logistics Information Management System
ATO	Authority to Operate	CGA	Coast Guard Academy
BCWP	Budgeted Cost of Work Performed	CGAP	Coast Guard Acquisition Process
BCWS	Budgeted Cost of Work Scheduled	CGBI	Coast Guard Business Intelligence
BOD	Business Operations Division	CGDN+	Coast Guard Data Network
BSD	Base Support Services Division	CGEA	Coast Guard Enterprise Architecture
C&A	Certification and Accreditation	CGMS	Coast Guard Messaging System
C2	Command and Control	CGONE	Coast Guard One Network
C21	Command 21	CIAO(s)	Commandant's Intent Action Order
C3CEN	Command and Control Engineering Center	CIM	Commandant Instruction Manual
C4	Command, Control, Communications, and Computers	CIO	Chief Information Officer
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance	CIRC	Computer Incident Response Center
C4IT	Command, Control, Communications, Computers, and Information Technology	CMMi	Capability Maturity Model Integration
CAC	Common Access Card	CMS	Content Management System
CAMSLANT	Communications Area Master Station Atlantic	CND	Computer Network Defense
CAMSPAC	Communications Area Master Station Pacific	COBIT	Control Objectives for Information and related Technology
		COE	Center of Excellence



COMDTINST	Commandant Instruction	EACOE	Enterprise Architecture Center of Excellence
CONOPS	Concept of Operations	EADS	Enterprise AIS Data Service
COOP	Continuity of Operations Planning	EAM	Enterprise Asset Management
COP	Common Operating Picture	EC	Engineering Change
CPIC	Capital Planning and Investment Control	eCG	Electronic Coast Guard
CPU	Central Processing Unit	EDC	Enterprise Data Catalog
CRRT	CIAO Reorganization Review Team	EDMO	Enterprise Data Management Office
CUI	Controlled Unclassified Information	EGMO	Enterprise Geospatial Management Office
DAA	Designated Accreditation Authority	eMICP	enhanced Mobile Incident Command Centers
DAC	Data Asset Catalog	ESB	Enterprise Service Bus
DCMS	Deputy Commandant for Mission Support	ESD	Engineering Services Division
DES	Data Encryption Standard	ESU(s)	Engineering Support Unit(s)
DGPS	Differential Global Positioning System	EVM	Earned Value Management
DHS	Department of Homeland Security	EXSTAGE	Execution Stage
DIACAP	Defense Information Assurance Certification and Accreditation Process	FDCC	Federal Desktop Core Configuration
DISA	Defense Information Systems Agency	FEMA	Federal Emergency Management Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process	FINCEN	Finance Center
DMS	Defense Messaging System	FISMA	Federal Information Security Management Act
DoD	Department of Defense	FOIA	Freedom of Information Act
DOG	Deployable Operations Group	FORCECOM	Force Readiness Command
DOJ	Department of Justice	FSAM	Federal Segment Architecture Methodology
DOORS	Dynamic Object Oriented Requirements System	FY	Fiscal Year
DRS	Disaster Recovery System	GCCS	Global Command and Control System
DSES	Directory Services and Exchange Services	GDC4S	General Dynamics C4 Systems
EA	Enterprise Architecture	GFE	Government Furnished Equipment
EAB	Enterprise Architecture Board	GIS	Geographic Information System
		GMT	Generally Mandated Training
		GOCO	Government Owned, Contractor Operated



GPS	Global Positioning System	LORAN	Long Range Aids to Navigation
HAS	Historical Archive System	LORSTA(s)	LORAN Station(s)
HF ALE	High Frequency Automatic Link Establishment	LRIP	Low Rate Initial Production
HR	Human Resources	MAP	Mission Action Plan
HRMS	Human Resources Management System	MCC	Mobile Command Center
HSPD	Homeland Security Presidential Directive	MCV	Mobile Communications Vans
IDP(s)	Individual Development Plans	MD	Management Directive
IA	Information Assurance	MDA	Maritime Domain Awareness
ICGS	Integrated Coast Guard Systems	MIEM	Maritime Information Exchange Model
IG	Inspector General	MILSATCOM	Military Satellite Communications
INCONUS	Intercontinental United States	MIPR	Military Interdepartmental Purchase Request
IOC	Initial Operational Capability	MIRP	Maritime Infrastructure Recovery Plan
IOC	Interagency Operation Center	MISLE	Maritime Information for Safety and Law Enforcement
IP	Internet Protocol	MLC(s)	Maintenance and Logistics Command(s)
IPv6	Internet Protocol Version 6	MMSI(s)	Maritime Mobile Service Incident(s)
IRB	Investment Review Board	MPLS	Multi-protocol Label Switching
ISC(s)	Integrated Support Command(s)	MOE	Measures of Effectiveness
IT	Information Technology	MOTR	Maritime Operational Threat Response Plan
ITAR	Information Technology Acquisition Review	MOA(s)	Memorandum of Agreement(s)
ITIL	Information Technology Infrastructure Library	MOTR	Maritime Operational Threat Response
ITU	International Telecommunications Unit	MOU(s)	Memorandum of Understanding(s)
IW	Integrated Waveform	MS EA	Microsoft Enterprise Agreement
KMF	Key Management Facility	MSAM	Major Systems Acquisition Manual
LAN	Local Area Network	MT&E	Maritime Test and Evaluation
LCMO	Life Cycle Management Organization	NAIS	Nationwide Automated Identification System
LIMS	Logistics Information Management System	NARA	National Archives and Records Administration
LoB	Line of Business	NIEM	National Information Exchange Model



NIPRNET	Unclassified but Sensitive Internet Protocol Router Network (formerly called the Non-Classified Internet Protocol Router Network)	PMO	Project Management Office
		PNT	Position Navigation and Timing
NIST	National Institute of Standards and Technology	PO&AM	Plan of Action and Milestones
		POC	Point of Contact
NLECC	National Law Enforcement Communications Center	PORD	Preliminary Operational Requirements Document
NMS	National Maritime Strategy	PPRB	Policy and Practice Review Board
NOC	Network Operations Center	PSB	Products and Standards Board
NSPD	National Security Presidential Directive	PTA	Privacy Threshold Analysis
		PTAs	Privacy Threshold Analyses
NSMS	National Strategy on for Maritime Security	Q1,2,3,4	Quarter one, two, three, four
OAP	Ocean Action Plan	R&D	Research and Development
OAS	Organizational Assessment Survey	RAP	Resource Allocation Plan
OCIO	Office of the Chief Information Officer	RAS	Remote Access Service
		RCC	Remote Control Console
OFCO	Operating Facility Change Order	RDC	Research and Development Center
OGAs	Other Government Agencies	RF	Radio Frequency
OIG	Office of the Inspector General	RFP	Request For Proposal
OMB	Office of Management and Budget	RSS	Real Simple Syndication
ORD	Operational Requirements Document	SAP	Stand-Alone Proxy
OSC	Operations Systems Center	SATCOM	Satellite Communications
OTAR	Over-the-air-rekeying	SBU	Sensitive But Unclassified
OUTCONUS	Outside the Continental United States	SDA	Systems Development Agent
		SDLC	Systems Development Life Cycle
PBX	Private Branch Exchange	SELC	Systems Engineering Life Cycle
PEP	Policy Enforcement Point	SETAB	Systems Engineering Technical Advisory Board
PHS	Public Health Service	SFLC	Surface Forces Logistics Center
PIA(s)	Privacy Impact Assessment(s)	SIPRNET	Secure Internet protocol Router Network
PII	Personally Identifiable Information		
PFD	Personnel and Facilities Division	SOA	Service Oriented Architecture
PM	Project Management	SOC	Security Operations Center
PMBok	Project Management Book of Knowledge	SOR	System of Record



SORN(s)	System of Record Notice(s)	VHF	Very High Frequency
SPAWAR	Space and Naval Warfare Systems Command	WAGB	Polar Class Icebreaker
SRCUS	Short-Range Communications Upgrade System	WAN	Wide Area Network
SSA	System Support Agent	WBS	Work Breakdown Structure
TASC	Transformation and Systems Consolidation	WHEC	Coast Guard High Endurance Cutter
TCM	Telecommunications Manual	WLB	Seagoing Buoy Tender
TCTO	Time Compliant Technical Order	WLI	Coast Guard Buoy Tender, Inland
TEAMS	The Enterprise Architecture Management System	WLIC	Inland Construction Tenders
TIC(s)	Trusted Internet Connection(s)	WLM	Coast Guard Buoy Tender, Coastal
TISCOM	Telecommunication & Information Systems Command	WLR	River Buoy Tender
TSA	Transportation Security Administration	WMEC	Coast Guard Medium Endurance Cutter
TTP	Tactics, Techniques, and Procedures	WMSL	National Security Cutter
UHF	Ultra High Frequency	WPB	Coast Guard Patrol Boat
USCG	United States Coast Guard	WPC	Patrol Coastal
USCGC	United States Coast Guard Cutter	WTGB	Coast Guard Icebreaking Tug
		WYTL	Small Harbor Tug
		XML	eXtensible Markup Language



## APPENDIX D: DEFINITIONS

### **Command, Control, Communications, Computers, and Information Technology**

Command, Control, Communications, Computers, and Information Technology (C4IT) consists of any equipment or interconnected system or subsystem of equipment, or technique used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of digital, voice, or video data or information to the appropriate levels of command. This includes command and control networks, common operational picture systems, information assurance services, communication products and standards, computers, ancillary equipment, software, firmware, procedures, services (including support services), and related resources.

### **Enterprise Architecture**

Enterprise Architecture (EA) is the discipline that synthesizes key business and technology information across the organization to support better decision-making. EA provides useful and usable information products and governance services to the end-user while developing and maintaining the current and target (to-be) architectures and transition plan for the organization. The information in the EA, includes: results of operations, business functions and activities, information requirements, supporting applications and technologies, and security.

### **Measure of Effectiveness**

A measure of effectiveness (MOE) is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.

### **Service Oriented Architecture**

Service Oriented Architecture (SOA) is a computer systems architectural style for creating and using business processes, packaged as services, throughout their lifecycle. SOA also defines and provisions the IT infrastructure to allow different applications to exchange data and participate in business processes. These functions are loosely coupled with the operating systems and programming languages underlying the applications. SOA separates functions into distinct units (services), which can be distributed over a network and can be



combined and reused to create business applications. These services communicate with each other by passing data from one service to another, or by coordinating an activity between two or more services. SOA concepts are often seen as built upon and evolving from older concepts of distributed computing and modular programming.

**Systems Development Life Cycle** The SDLC is a sequence of seven phases used to produce, operate, and support C4IT systems. These phases begin with the identification of need and span all facets of a C4IT system's life cycle, including planning, acquisition, deployment, operation, and retirement of a system. The SDLC Practice is based on industry and government best practices and shall be kept current through updates to the SDLC Practices. SDLC Practices shall be promulgated separately and shall identify inputs, outputs, procedures, and products for each phase. For more information about the Coast Guard's SDLC process, see COMDTINST 5230.66.



## APPENDIX E: REFERENCES

Department of Defense (2007). *Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms"*. As amended through 17 October 2007. Retrieved 20 March 2008, from <http://www.dtic.mil/doctrine/jel/doddict/>

Department of Homeland Security (2004). *Securing Our Homeland, U.S. Department of Homeland Security Strategic Plan*.

Department of Homeland Security (2007). *Office of the Chief Information Officer Strategic Plan: Fiscal Years 2007-2011*.

Executive Office of the President (2005). *The National Strategy for Maritime Security*. Retrieved 21 May 2008, from <http://www.whitehouse.gov/homeland/maritime-security.html#intro>.

Executive Office of the President (2007). *The National Strategy for Homeland Security*. Retrieved 21 May 2008, from <http://www.whitehouse.gov/homeland/maritime-security.html#intro>.

Kurzweil, Ray (2001). *Essay: The Law of Accelerating Returns*. Retrieved 30 March 2008, from <http://www.kurzweilai.net/meme/frame.html?main=/articles/art0134.html>.

U.S. Coast Guard. *Commandant's Intent Action Orders*.

U.S. Coast Guard (2007). *The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship*.

U.S. Coast Guard (2008). *The U.S. Coast Guard Enterprise Architecture Executive Handbook*. Retrieved 15 May 2008, from <http://cgea.uscg.mil/>





