2012 Clinger-Cohen
Core Competencies & Learning Objectives

December 2012

Contents

Introduction

The Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act and now codified in title 40 of the United States Code) created a wide array of responsibilities for federal agency Chief Information Officers, including developing strategies and specific plans for hiring, training and professional development of the information technology (IT) workforce. In 1997, the first iteration of the Clinger-Cohen Core Competencies was published to create a baseline of information resources management knowledge requirements. Learning objectives were added in 1999 to identify the level of performance desired to be mastered within an academic or experiential environment.

Periodically, the Federal Government reviews this core body of competencies in order to ensure critical knowledge areas impacting information resources management are captured. Changes reflect new statutory and regulatory requirements, as well as areas requiring greater emphasis due to new policies and strategies (e.g., the recently released presidential strategy on Digital Government), continuous changes in technology, and other evolving agency IT/cybersecurity mission requirements. In 2012, new competencies were added for IT Governance, IT Program Management Leadership, Vendor Management, Cybersecurity/Information Assurance Strategies and Plans, Social Media, Cloud Computing, Open Government, Information Collection, and Information Accessibility. Administratively, references were updated and summarized in a separate appendix, and language was streamlined in accordance with the Plain Writing Act of 2010.

The review process was a collaborative effort among 12 federal agencies, academic representatives from the CIO University Consortium, and members from the Industry Advisory Council and federally funded research community and was led and managed by the IT Workforce Committee of the CIO Council.

The 2012 Clinger-Cohen Core Competencies and their associated learning objectives will be used as the foundation for IT course and curriculum development, as well as the development and consistent implementation of IT workforce policy initiatives across the Federal Government. This effort fulfills IT workforce management requirements set forth in Subtitle III of title 40 of the United States Code (U.S.C.) (Clinger-Cohen Act of 1996) and title II of Public Law 107-347 (E-Government Act of 2002, 44 U.S.C. 3501 note).

2012 Clinger-Cohen Core Competencies and Learning Objectives

The Clinger-Cohen Core Competencies reflect a core body of 12 competency areas identified by the Federal CIO Council as fundamental to the effective management of federal technology resources: Policy and Organization; Leadership and Human Capital Management; Process and Change Management; Information Resources Strategy and Planning; IT Performance Assessment: Models and Methods; IT Project and Program Management; Capital Planning and Investment Control; Acquisition; Information and Knowledge Management; Cybersecurity/Information Assurance; Enterprise Architecture; and Technology Management and Assessment. Each of the 12 competency areas has several subordinate competencies and all subordinate competencies have associated learning objectives.

The learning objectives form the foundation for curriculum development by the educational institutions offering approved programs under the CIO University Consortium umbrella. The objectives identify key concepts and capabilities to be taught and can also be used as a professional development guideline for both individuals and organizations. Each individual's professional development roadmap can be achieved through a variety of methods, including formalized academic programs, mentoring, on-the-job training, professional details, and prior experiential assignments.

It is not expected than any one individual would master all management activities contained within these competencies. Areas of concentration would reflect individual job requirements, as well as personal development interests. Additionally, specific technical expertise outside the scope of these competencies may be required based on actual job roles. Federal Chief Information Officers should ensure that the knowledge, skills and abilities represented in each competency in this document are resident within their organization for overall staff productivity.

References listed next to selected learning objectives are designed to guide the learning process but should not be considered all-inclusive. The references cited reflect pertinent statutes, regulations, and policy associated with the given subject matter that are particularly relevant for federal IT employees. A complete listing of references is included in Appendix A.

Finally, individual learning objectives have been mapped to the Office of Personnel Management's Executive Core Qualifications (ECQ) where applicable. Attainment of these qualifications is required for entry to the Senior Executive Service. The mapping is provided to support multi-purpose leadership development for IT management and executive positions.

Clinger-Cohen Core Competencies	Learning Objectives
1.0: Policy and Organization	*General Discussion: The CIO has one of the most cross-cutting positions in government and must be able to work effectively with a wide range of people across multiple organizations. Additionally, the CIO must be comfortable in a fast-changing environment that includes evolving technologies, legislation, policy, and politics.*
Competency 1.1 - Department/Agency missions, organization, functions, policies, and procedures	1.1 LO 1: Describe the varied interpretations of information technology (IT) (e.g., systems data, related peripherals and services); IT focus (operational vs. technical); and IT's typical use in organizational structures.
	1.1 LO 2: List and describe the elements of the CIO's role that are common to all CIOs regardless of their organization's size.
	1.1 LO 3: Define the CIO's role in the Federal Government including: (1) leadership of the IT organization/community; (2) oversight role associated with IT governance; and (3) valued member of the Department's senior leadership team. (See also Competency 1.6 on IT governance.)
	1.1 LO 4: Compare different agency CIO organizational structures against general models available. (See also 1.4 LO 2.)
• OPM ECQ 1	1.1 LO 5: Using metrics where possible, identify and discuss the environment, attributes, and best practices that characterize an effective CIO organization.
• OPM ECQ 1	1.1 LO 6: Compare an IT strategic plan with an overarching agency plan and determine performance gaps. (See also 5.1 LO 4 and 5.1 LO 6.)

Competency 1.2 - Governing laws and authorities • 5 U.S.C. 552 and 552a • 6 U.S.C. 485 • 29 U.S.C. 794d • Chapters 31, 35 and 36 of Title 44, U.S.C. • 40 U.S.C. Subtitle III • E-Government Act • GPRA Modernization Act of 2010 • EO 13231 • EO 13526 • EO 13556 • EO 13576 • OMB Circular A-11 • OMB Circular A-123 • OMB Circular A-130 • HSPD 7 • HSPD 12 • OPM ECQ 1	1.2 LO 1: Identify current and emerging legislation, regulations, and policies relevant to the CIO's responsibilities. Assess their provisions, including performance mandates, and discuss their organizational implications. (See also 5.1 LO 1.)
• OPM ECQ 1, 5	1.2 LO 2: Discuss how regulatory, oversight, and interagency policy groups impact a CIO's responsibilities and organization.
• ISO 38500 • ISO/IEC 27000 series • OPM ECQ 5	1.2 LO 3: Discuss the importance of standards issued by organizations such as the National Institute of Standards and Technology (NIST); the American National Standards Institute (ANSI); and the International Organization for Standardization (ISO) and their impact on the IT business environment.
	1.2 LO 4: Discuss the applicability of governing laws and authorities to contractor-managed/hosted systems and/or websites.
	1.2 LO 5: Discuss IT capability to track, evaluate and communicate emerging legislation, regulations, and intergovernmental legislation, including changes in acquisition regulations/guidelines.

Competency 1.3 - Federal government decision and policy-making processes • OMB Circular A-11 • OPM ECQ 1	1.3 LO 1: Discuss the IT strategic planning process. Identify internal and external drivers; organizational strengths, weaknesses, and culture; and future trends.
• OPM ECQ 1	1.3 LO 2: Apply a strategic planning process that crosswalks IT/CIO, enterprise-wide, and government-wide strategies, strategic goals, and performance objectives.
• OPM ECQ 1	1.3 LO 3: Discuss the advantages and limitations of different decision-making approaches. (See also 2.1 LO 11.)
• OPM ECQ 1	1.3 LO 4: Describe approaches needed to develop a supportive climate for IT innovation and provide examples of successful applications in government.
• OPM ECQ 1	1.3 LO 5: Identify evaluation methods and metrics to assess the CIO's effectiveness in supporting an agency's strategic plan.
Competency 1.4 - Linkages and interrelationships between Agency heads and their Chief Executive Officers	1.4 LO 1: Describe the roles of the Agency head, the various Chief Executive Officers (CXOs), and their interrelationships.
	1.4 LO 2: Discuss and analyze organizational structure and interaction, line and staff responsibilities, the flow of communications, independent and interdependent decision-making, and the contribution of IT and the CIO to the organizational structure, using a systems perspective. (See also 1.1 LO 4.)
	1.4 LO 3: Map the structure and the information flows of a CIO organization.

Competency 1.5 - Intergovernmental programs, policies, and processes	1.5 LO 1: Discuss the legislative, regulatory and coordination dimensions and mechanisms of intergovernmental programs, policies and processes. (Also see Competency 7.5.)
• 6 U.S.C. 485 • EO 13388 • PPD-1 • OMB M-11-02 • OPM ECQ 5 • U.S. Intelligence Community, Information Sharing Policy • National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information Sharing	1.5 LO 2: Analyze the role of the CIO and the challenges associated with implementing effective internal and external agency information sharing. Include an examination of the laws, regulations and policies; technical issues; procedural obstacles; and cultural barriers. (Also see 3.5 LO 1 and 10.4 LO 2.)
• OPM ECQ 5	1.5 LO 3: Analyze government partnership opportunities enabled by technology that can assist the CIO in achieving mission requirements.
• Federal Advisory Committee Act • OMB Circular A-135 • OPM ECQ 5	1.5 LO 4: Discuss how government-wide policy groups and advisory groups impact agency operations.
• OPM ECQ 5	1.5 LO 5: Discuss the significance of management oversight, both internal and external (e.g., Congress, the Office of Management and Budget (OMB), the General Accountability Office (GAO), and the Office of the Inspector General (OIG)), and effective methods to create an open, ongoing dialogue between these entities and the CIO organization.
Competency 1.6 - IT governance • 44 U.S.C. 3603 • OMB M-09-02 • OMB M-11-29 • Federal CIO Council Charter • ISO 38500	*General Discussion: IT is an integral part of agency's overall governance and consists of the leadership and organizational structures and processes that ensure that the agency's IT sustains and extends the agency's mission by supporting its information management and delivery needs. CIOs not only must be a part of the overall agency governance, but also must ensure that they have functioning governance mechanisms for policy making, enforcement and decision making on IT issues that are effective, transparent, and accountable.*

	1.6 LO 1: Review the overall agency governance structure to determine where the CIO participates and with what kind of authority.
	1.6 LO 2: Identify where the CIO derives his/her authority – statutorily directed or by delegation – to participate in the agency's major decision making processes – namely, budgeting, requirements development, and acquisition.
	1.6 LO 3: Discuss the advantages and disadvantages of the CIO's role on various agency governance bodies.
	1.6 LO 4: Discuss the role of CIOs in other agencies' governance structures.

2.0: Leadership and Human Capital Management	*General Discussion: Management concepts are important <u>but</u> CIOs must move beyond management to leadership. This includes oversight over the individuals within their organization, and working to attract, retain, and develop their personnel.*
Competency 2.1 - Key CIO leadership attributes • OMB M-09-02 • OMB M-11-29 • OPM ECQs 1-5	2.1 LO 1: Compare the various roles and skills of a CIO with the Office of Personnel Management's listing of Executive Core Qualifications that all CIOs are expected to demonstrate.
	2.1 LO 2: Discuss the importance of CIOs identifying their own interpersonal skill sets, as well as those of their staff.
	2.1 LO 3: Compare and contrast different leadership styles and how effective they are in a CIO organization.
• OPM ECQ 1	2.1 LO 4: Discuss the relationship between program visionary leadership and technical visionary leadership and the need for both.
	2.1 LO 5: Define the communication process, and give examples of effective communication skills.
	2.1 LO 6: Identify and demonstrate behaviors related to effective listening and feedback.
	2.1 LO 7: Discuss barriers to communications in an interconnected world, and approaches to overcome and/or manage them.
	2.1 LO 8: Describe the range and effect of interpersonal communications (including media) in individual, small group, and organizational communication.
	2.1 LO 9: Discuss and demonstrate the application of the principles of individual behavior and group behavior in organizations.
	2.1 LO 10: Evaluate both need-based theories of motivation and process-based theories. Illustrate how to apply these theories in the workplace.
	2.1 LO 11: Discuss the advantages and limitations of different decision-making approaches, and identify methods of effective decision-making that support the specific agency mission of the CIO. (See also 1.3 LO 3.)
• OPM ECQ 2	2.1 LO 12: Describe the role of conflict in an organization and demonstrate effective conflict management skills.
• OPM ECQ 3	2.1 LO 13: Design approaches to champion initiatives.

Competency 2.2 - Professional development and career planning • 40 U.S.C. 11315 • 44 U.S.C. 3506 • OMB Circular A-130 • OPM ECQ 2	2.2 LO 1: Discuss the role of the CIO in creating and maintaining a supportive infrastructure for staff personal and professional development. Include in the discussion the responsibilities of managers and supervisors.
• OPM ECQ 2	2.2 LO 2: Identify approaches to maintain continuous learning to support mission critical competencies.
• OPM ECQ 2	2.2 LO 3: Discuss how to build a training program that recognizes and accommodates different learning styles.
• OPM ECQ 2	2.2 LO 4: Discuss different workforce organizational developmental tools, including the use of gap analysis. (See also 3.0 LO 1.)
• OPM ECQ 2, 4	2.2 LO 5: Analyze a variety of methods to establish IT career development paths and programs in government.
• OPM ECQ 2, 4	2.2 LO 6: Discuss the effectiveness of various staff recruitment, development and retention plans. (Also see Competency 2.6 on Attracting and retaining personnel.)
• OPM ECQ 4	2.2 LO 7: Discuss how to conduct succession planning in an organization.
• OPM ECQ 2, 4	2.2 LO 8: Discuss how to integrate generational differences in workforce planning and professional development programs.
Competency 2.3 - Competency performance and management	2.3 LO 1: Describe how IT certifications, testing, and academic degrees are used to build competency strength in the Federal Government.
	2.3 LO 2: Discuss how to create position descriptions and competency selection criteria that align to your agency's organizational design.
	2.3 LO 3: Identify and discuss positions, particularly those impacting IT, for which there are legislated or regulated competency requirements (e.g., IT acquisition, cybersecurity/IA, IT program/project management).
	2.3 LO 4: Compare and contrast methods to evaluate competency performance.
Competency 2.4 - Partnerships and team-building • OPM ECQ 2	2.4 LO 1: Discuss Organizational Development techniques and their role in team building and partnering. (See also 3.1 LO 1.)
• OPM ECQ 2	2.4 LO 2: Discuss the principles of group dynamics and how

	they can assist a manager in anticipating behavior.
• OPM ECQ 2	2.4 LO 3: List and define typical integrated project team roles.
• OPM ECQ 2	2.4 LO 4: Describe the team-building process, including the need for trust and the importance of empowerment.
• OPM ECQ 2	2.4 LO 5: Discuss and apply the principles of team leadership in a variety of settings including a matrix environment, an inter-organizational environment, and a systems environment.
• OPM ECQ 2	2.4 LO 6: Evaluate the contributions that self-awareness tools bring to team-building.
• OPM ECQ 2	2.4 LO 7: Discuss the dynamics of managing a team when alternative work sites and flexible work schedules are employed within the organization.
• OPM ECQ 2	2.4 LO 8: Discuss the challenges of vendor integration into team projects. (See also 6.8 LO 3.)
• OPM ECQ 2	2.4 LO 9: Identify appropriate team-building approaches to be used in multi-disciplinary, inter-organizational, and partnership situations.
• OPM ECQ 5	2.4 LO 10: Describe the technical and cultural challenges of cross-boundary and interagency partnering. (See also Competency 3.5 on Cross-boundary collaboration.)
Competency 2.5 - Personnel performance management • OPM ECQ 4	2.5 LO 1: Evaluate advantages and disadvantages of different performance management and appraisal approaches.
• OPM ECQ 4	2.5 LO 2: Discuss proven methods of communicating job expectations.
• OPM ECQ 4	2.5 LO 3: Discuss how to engage staff members in establishing their performance objectives.
• OPM ECQ 4	2.5 LO 4: Justify the value of timely performance feedback, and generational perspectives on desired frequency.
• OPM ECQ 3	2.5 LO 5: Describe the role of accountability in creating a results-driven organization.
• OPM ECQ 4	2.5 LO 6: Discuss how the implementation of Competency 2.5, learning objectives 1 through 5, prepares managers to effectively address poor performance.

Competency 2.6 – Attracting, motivating, and retaining IT personnel • OPM ECQ 4	2.6 LO 1: Discuss the role that encouragement, empowerment, recognition and frequent performance feedback play in employee engagement and retention. (See also 2.2 LO 6.)
• OPM ECQ 2, 4	2.6 LO 2: Describe the ways in which a culture of trust functions as a motivator, encourages innovation, and retains personnel.
• OPM ECQ 2	2.6 LO 3: Design approaches to develop and implement a culture of trust.
• OPM ECQ 2	2.6 LO 4: Discuss the opportunities and challenges present in a workplace that exhibits diversity of all kinds, including, but not limited to, gender, race, creed, sexual orientation, national origin and generational differences.
• OPM ECQ 4	2.6 LO 5: Describe how a clearly defined and jointly held vision improves personnel recruiting, retention and performance.
• OPM ECQ 4	2.6 LO 6: Discuss the importance of professional development opportunities and career management support in creating an attractive work environment for potential and current employees.
	2.6 LO 7: Explain how lack of resources can impact job satisfaction, employee engagement and the achievement of organizational mission.
• OPM ECQ 2, 4	2.6 LO 8: Review best practices for acquiring, developing and retaining high caliber, multi-generational IT professionals.

3.0: Process and Change Management	*General Discussion: The paramount role of the CIO is as Chief Visionary of the organization's information and technology—critical enablers for achieving mission and improving efficiency. Change management encompasses far more than a single leader's perspective. The CIO works in strong partnership with the CXOs and other key stakeholders as part of the change management process. Open, effective communications are essential to ensure organizational buy-in.*
• OPM ECQ 1	3.0 LO 1: CIOs frequently must lead change (technology adoption, skill transfer, etc.) in an organization. Discuss the concept of change, and the dimensions of behavioral change. (See also 2.2 LO 4 and 2.4 LO 1.)
• OPM ECQ 1	3.0 LO 2: Discuss the role of leadership, including that of the CIO, in successful change initiatives.
• OPM ECQ 1, 3	3.0 LO 3: Justify the importance of stakeholder "buy-in" in successful change efforts.
	3.0 LO 4: Identify and demonstrate approaches a CIO can use to achieve stakeholder support in change efforts.
	3.0 LO 5: Federal CIOs work within a large system that includes the Office of Management and Budget, the Federal CIO Council, and different administrations, executing multiple initiatives that continuously require changes. Discuss the dimensions of the government environment as a factor in successful change management.
Competency 3.1 - Organizational Development	*General Discussion: It is important that CIOs be familiar with Organizational Development (OD) concepts and OD's importance as an independent discipline. CIOs need to be able to critically assess the organization against strategic goals, be familiar with the tenets of change management, and assess planned change from a systems perspective*.
	3.1 LO 1: Discuss the concepts and methods of Organizational Development. (See also 2.4 LO 1.)
• OPM ECQ 1	3.1 LO 2: Discuss organizational assessment methods and metrics used to assess the need for change.
• OPM ECQ 1	3.1 LO 3: Describe various change techniques and tools.
• OPM ECQ 1	3.1 LO 4: Design approaches (including the identification of key influential individuals) to prepare the workplace for change.
• OPM ECQ 1	3.1 LO 5: Discuss organizational resistance to change, including the identification of barriers and strategies for overcoming resistance.

• OPM ECQ 1	3.1 LO 6: Differentiate between voluntary and mandated change strategies and the approaches to their implementation.
• OPM ECQ 1	3.1 LO 7: Design a comprehensive plan to implement, communicate, and champion an organizational change initiative.
Competency 3.2 - Process management and control	3.2 LO 1: Discuss the principles of process management and control.
	3.2 LO 2: Compare, contrast and evaluate the major tools, techniques and methods of process management.
	3.2 LO 3: Describe gap analysis and how to apply its results within an organization.
	3.2 LO 4: Evaluate the importance of internal control systems within the CIO organization.
Competency 3.3 - Quality improvement models and methods	3.3 LO 1: Explain the different uses and meanings of the term “quality.”
	3.3 LO 2: Assess and prioritize quality factors used in business, information and technical areas.
	3.3 LO 3: Discuss the dimensions of quality when addressing customer, employee and stakeholder expectations.
• OPM ECQ 3	3.3 LO 4: Discuss how quality can be integrated into the culture of the organization.
	3.3 LO 5: Discuss how to integrate quality dimensions into strategic planning, performance goals and objectives.
• OPM ECQ 3	3.3 LO 6: Describe the CIO's responsibilities regarding quality improvement.
	3.3 LO 7: Compare and contrast programs and standards associated with quality management. Include in the discussion ISO 9001 and 20000, the Baldrige Award, Quality Function Deployment (QFD), Capability Maturity Model Integration (CMMI), and the Information Technology Infrastructure Library (ITIL).
Competency 3.4 - Business process redesign/reengineering models and methods	3.4 LO 1: Define Business Process Improvement, redesign, and reengineering (BPI/BPR).
	3.4 LO 2: Trace and assess the history, evolution, and relationships of Business Process Reengineering (BPR), Business Process Improvement (BPI), and other business process transformation initiatives.
	3.4 LO 3: Discuss examples of successful BPI, redesign, and BPR initiatives within government.

	3.4 LO 4: Discuss the models and methods that may be used in a comprehensive BPI effort. Include discussion of continuous process improvement tools and evaluate their benefits.
	3.4 LO 5: Discuss the unique challenges associated with undertaking business process re-design.
	3.4 LO 6: Identify the key management actions required to manage a portfolio of process improvement initiatives across the enterprise.
	3.4 LO 7: Design an integrated management approach to support embedding and institutionalization of process changes in organizations.
Competency 3.5 - Cross-boundary process collaboration • OPM ECQ 5	3.5 LO 1: Discuss inter-agency, industry and academic collaboration initiatives and best practices, including common process languages, collaborative technology interfaces and common process standards. (See also 1.5 LO 2 and 2.4 LO 10.)
• OPM ECQ 5	3.5 LO 2: Identify cultural challenges a CIO may face in cross-boundary, inter-agency collaborations.
• OPM ECQ 5	3.5 LO 3: Examine business cases that highlight the successes and failures of inter-agency collaboration efforts.

4.0: Information Resources Strategy and Planning	*General Discussion: IT must be a value-adding dimension of the business plan. Information Resources Management (IRM) strategic planning must begin with the business strategic planning process and integrate with the organization's business functions and plans since business planning and IRM planning are parallel and coupled processes. IRM planning should also address cross-governmental and inter-agency planning issues as well as external drivers.*
• OPM ECQ 1	4.0 LO 1: Describe the principles of strategic planning as they apply to IT.
	4.0 LO 2: Describe the relationship between IT strategic planning and IT functional analysis.
• OPM ECQ 1	4.0 LO 3: Describe how IT visionary strategic planning is linked to enterprise/program visionary strategic planning.
Competency 4.1 - IRM baseline assessment analysis	4.1 LO 1: Define and describe performance goals and distinguish performance goals from performance standards.
	4.1 LO 2: Discuss benchmarking, particularly as applied to IT hardware, software, networking (e.g., protocols) and IT staff skills and abilities.
	4.1 LO 3: Evaluate a current baseline analysis against established benchmarks.
	4.1 LO 4: Describe the ways in which benchmarks may be used to forecast performance.
	4.1 LO 5: Explain the importance of IT performance assessment and analysis, and summarize how results can be used to develop IRM strategies and plans that support mission objectives and business goals.
	4.1 LO 6: Design performance analysis and assessment approaches that address each element of an IT organization.
	4.1 LO 7: Discuss the baseline review and the development of total cost of ownership estimates. Include correlation to enterprise architecture, capital planning and investment and systems development lifecycle.
Competency 4.2 - Interdepartmental, inter-agency IT functional analysis	4.2 LO 1: Define functional analysis in an IRM setting.
	4.2 LO 2: Define the purpose and goals of IT functional analysis. Discuss when cross-functional work is desirable and when it is not desirable.
	4.2 LO 3: Using a mission statement and baseline analysis, analyze the functional and cross-functional requirements for an IT group.

	4.2 LO 4: Using an example of an interagency IT partnership, assess the potential challenges resulting from scope expansion.
	4.2 LO 5: List and describe functional analysis issues (e.g., security, privacy, accessibility, and open access). (See also 9.2 LO 1.)
	4.2 LO 6: Compare and contrast various potential solutions to IT needs, including, "Use what we've got. Build new. Acquire from the private sector. Acquire from the public sector," etc.
	4.2 LO 7: Discuss the statement that "cross-functional IT aspects must be embedded in the system." Include the communication channels (interdepartmental, interagency, and intergovernmental) appropriate to the level of discussion.
Competency 4.3 - IT planning methodologies	4.3 LO 1: List and describe a comprehensive IT planning process.
	4.3 LO 2: Compare and contrast the range of IT planning methodologies, including gap analysis, weighted priorities, modeling techniques, Capability Maturity Modeling, Business Process Improvement and Business Process Reengineering.
Competency 4.4 - Contingency and continuity of operations planning (COOP) • NSPD-51/HSPD-20 • NCSD 3-10 • FCD 1 and 2 • OMB Circular A-130, Appendix III • NIST SP 800-34	4.4 LO 1: Discuss the need for contingency plans to protect against costly IT events caused by manmade activities and natural disasters; include discussion of potential risks and how to prioritize them.

	4.4 LO 2: Discuss the challenges of garnering the needed resources to protect against costly IT events.
	4.4 LO 3: Discuss the value of interoperability of resources in support of contingency needs.
	4.4 LO 4: Discuss the benefits of periodically reviewing IT contingency plans.
	4.4 LO 5: Develop a mock COOP with policies, procedures, plans and annual testing and reporting requirements to ensure the continuity of operations for an agency's information systems.
	4.4 LO 6: Evaluate (test) a plan to ensure the continuity of operations for information systems that support the operations and assets of an agency.
Competency 4.5 - Monitoring and evaluation methods and techniques	4.5 LO 1: Describe methods to assess the value, benefit and cost of IT and its impact on the organization.
	4.5 LO 2: Discuss the value of Activity Based Costing (ABC) in demonstrating the value and benefits of IT.
	4.5 LO 3: Describe and evaluate the applicability of frameworks such as Capability Maturity Model Integration (CMMI), ISO 9001, the Information Technology Infrastructure Library (ITIL) and Control Objective over Information and Related Technology (COBIT).
	4.5 LO 4: Describe and evaluate the strengths and weaknesses of qualitative and quantitative data collection techniques including interviews, elite interviews, focus groups, surveys, questionnaires, etc. Include discussion of reliability and validity of survey data.
	4.5 LO 5: Discuss the use of questionnaires and other survey instruments for operational analysis, addressing customer satisfaction and identifying qualitative gaps that may exist in IT services. (See also 5.6 LO 3.)

5.0: IT Performance Assessment: Models and Methods	*General Discussion: The CIO has the challenge of meeting both customer and organizational needs established in the agency's business plan. In order to ensure those needs are being met, the CIO must understand the importance of the qualitative and quantitative baseline assessment measures and their use in the performance assessment cycle.*
Competency 5.1 - Government Performance and Results Act (GPRA) and IT • 5 U.S.C. 552 and 552a • 29 U.S.C. 794d (Section 508 of the Rehabilitation Act of 1973, as amended) • Subtitle III of Title 40, U.S.C. • Chapters 31, 35 and 36 of Title 44, U.S.C. • Chapter 9 of Title 31, U.S.C. (Chief Financial Officers Act of 1990) • E-Government Act • GPRA Modernization Act of 2010 • Presidential Memo, Transparency and Open Government • EO 13576 • OMB M-09-12 • OMB M-11-17 • OMB M-11-29 • OMB, 25 Point Implementation Plan to Reform Federal Information Technology Management	5.1 LO 1: List current federal performance legislation and describe/discuss the performance mandates that a CIO must address. (See also 1.2 LO 1.)
	5.1 LO 2: List and describe qualitative contributions to business value including usability, accessibility, efficiency, productivity and perceived value.
• OMB M-11-26 • OMB M-12-10 • OMB M-12-20 • OMB Circular A-11	5.1 LO 3: Illustrate sources of data that can be used to support performance assessment conclusions and decisions.
• OPM ECQ 1	5.1 LO 4: Describe how IT strategic planning relates to the business mission, vision, strategy, goals and objectives of an organization. (See 1.1 LO 6.)
• OPM ECQ 1	5.1 LO 5: Describe how IT initiatives support the goals within an IT strategic plan.
• OPM ECQ 1	5.1 LO 6: Develop an IT strategic plan that is integrated with

	organization mission objectives, business goals, and target architecture. (See 1.1 LO 6 and 11.3 LO 6.)
• OPM ECQ 3	5.1 LO 7: Determine how best to identify key external and internal IT stakeholders and customers and how to interface with each for optimum results.
Competency 5.2 - System development decision making	5.2 LO 1: Identify criteria to be used when analyzing whether to replace an existing system.
	5.2 LO 2: Describe best practices for identification and documentation of stakeholder requirements related to the development of a potential new system.
	5.2 LO 3: Compare and contrast the characteristics and the challenges involved in "new" systems, both those that are replacing existing systems, and those that are completely new.
	5.2 LO 4: Identify criteria and integrate "go/no go" checkpoints into a development lifecycle.
	5.2 LO 5: List and describe the decision tools and evaluation systems that are typically used to make go/no go decisions.
	5.2 LO 6: Identify and evaluate the criteria required to determine whether to "stop" or "kill" a project.
Competency 5.3 - Measuring IT success	5.3 LO 1: List and explain criteria used to determine IT success in meeting stakeholder needs, customer needs and mission performance.
	5.3 LO 2: Define the terms measure, milestone, metric and objective and their functions in measuring success.
	5.3 LO 3: Describe the differences between leading and lagging indicators and give examples of both.
	5.3 LO 4: Discuss the need for measurements, the limits of analysis, and the hazards of measurement for measurement's sake.
	5.3 LO 5: Distinguish between outcome (what the system needs to achieve) and output (what the system does) in defining performance measures.
	5.3 LO 6: Discuss the importance of identifying a few critical measures of IT success, and how to keep them visible.
	5.3 LO 7: Demonstrate the value of continuous assessment of IT strategic plan milestones.

Competency 5.4 - Defining and selecting effective performance measures	5.4 LO 1: List, describe, and evaluate techniques that are appropriate for measuring effective performance. Identify where these techniques may be found. Include in the discussion the Goals, Questions, Metrics, Measures (GQMM) approach, the Balanced Scorecard, Benchmarking, Best Practices, and OMB Circular A-11.
• OPM ECQ 3 • OMB M-11-26 • OMB M-12-10 • OMB M-12-20 • OMB Circular A-11 • OMB Guidance on Exhibit 300	5.4 LO 2: Describe how to choose performance measures that align with stakeholder needs, mission, vision, critical success factors, etc.
• OPM ECQ 3	5.4 LO 3: Discuss the advantages and disadvantages of building user feedback into the design and development of performance measures.
Competency 5.5 - Evaluating system performance • OMB M-11-26 • OMB M-12-10 • OMB Circular A-11 • OMB Guidance on Exhibit 300	5.5 LO 1: Identify, evaluate and report on sources of performance evaluation information including internal databases, government-wide databases, proprietary databases, and available web sites.
	5.5 LO 2: Discuss how to evaluate whether technology is fulfilling strategic mission objectives and business needs as well as the tactical dimensions of service, information and system quality.
• OPM ECQ 3	5.5 LO 3: Discuss the approaches to, and the value of, identifying and prioritizing customers and stakeholders.
Competency 5.6 - Managing IT reviews and oversight processes • OMB M-11-26 • OMB M-12-10 • OMB M-12-20 • OMB Circular A-11 • OMB Guidance on Exhibit 300	5.6 LO 1: Discuss the significance and impact of both internal and government-mandated IT reviews.
	5.6 LO 2: Define the roles and responsibilities of managers (program managers, project managers, program leads, etc.) in the IT review process.
	5.6 LO 3: Identify key performance parameters for each phase in the lifecycle, using a specified project plan. (See also

	4.5 LO 4.)
	5.6 LO 4: Design a method to ensure that data collected in the assessment process is used in the review and decision making processes.

6.0: IT Project and Program Management	*General Discussion: The relationship between project management and program management is interdependent, not discrete, and progressively cumulative. A project is a specific investment having defined goals, objectives, requirements, lifecycle cost, a beginning and an end that delivers a specific product, service or result. A program is typically a group of related work efforts, including projects, managed in a coordinated way. Programs usually include elements of ongoing work. For program management processes to be mature, project management processes must be mature. IT Program Managers should be skilled in both IT Project and IT Program Management Competencies*
• ANSI/PMI 99-001-2008 • Project Management Book of Knowledge	6.0 LO 1: Describe the elements included in the project management lifecycle, including initiation, planning, execution, controlling and monitoring, and closing.
	6.0 LO 2: Discuss the CIO's lifecycle responsibility for IT project and program management.
	6.0 LO 3: Examine the importance of ethics, integrity, objectivity and accountability in IT project and program management.
• ANSI/PMI 99-001-2008	6.0 LO 4: Explore sources of project management standards.
• OMB M-04-19 • OMB M-11-29 • OMB Guidance on Exhibit 53 • OMB Guidance on Exhibit 300 • OFPP Policy Memo on FAC-P/PM dtd April 25, 2007	6.0 LO 5: Examine federal IT project and program manager qualification requirements and their impact on agency operations.
Competency 6.1 - Project scope and requirements management	6.1 LO 1: Using a case study, analyze the business or mission needs that are driving project requirements.
	6.1 LO 2: List and define the elements involved in the scope (money, time, people, impact, etc.) of a specified project or program being considered.
	6.1 LO 3: Discuss the ways in which project requirements affect project scope and scope management.
	6.1 LO 4: Discuss how the project or program scope elements link to organizational mission and goals.
	6.1 LO 5: Assess potential positive and negative effects that arise from change (mission, organizational structure, organizational resources, etc.).
	6.1 LO 6: Discuss and design approaches to both track and control project requirements, technology changes, and user

	needs changes.
• NIST SP 800-128	6.1 LO 7: Discuss approaches to configuration management and develop procedures for establishing and maintaining a Configuration Control Board (CCB). (See also 9.6 LO 4.)
	6.1 LO 8: Illustrate how poor requirements management may cause scope creep.
	6.1 LO 9: Evaluate the decision-making methods and tools (both macro and micro) and analyze the outputs they make available to the project/program manager.
	6.1 LO 10: Discuss the implications of rapid design modeling techniques and methods on requirements and scope management. Include discussion on use of pilots and prototypes.
	6.1 LO 11: Describe the relevant functional requirements contained in DoD 5015.2-STD, "Design Criteria for Electronic Records Management Software Applications" and discuss their impact on system design and implementation.
Competency 6.2 - Project integration management	6.2 LO 1: Define and illustrate project integration and implementation.
	6.2 LO 2: Develop plans to integrate project management and business management.
	6.2 LO 3: Establish software management approaches to include promotion of process improvements, commercial off-the-shelf (COTS) risk assessment, human systems integration design and applications security analysis.
	6.2 LO 4: Discuss and give examples of the importance of innovation and creative thinking in creating alternate program integration strategies.
	6.2 LO 5: Describe integration across programs including the reallocation of resources.
	6.2 LO 6: Compare, contrast and evaluate available Knowledge Management tools.
	6.2 LO 7: Assess the value of electronic communication tools as an integration driver.
Competency 6.3 - Project time, cost, and performance management	6.3 LO 1: Discuss concepts of project planning, such as Work Breakdown Structure (WBS) development and critical path analysis and their relationship to project delivery.
• OMB M-10-27 • GAO-09-3SP	6.3 LO 2: Describe and evaluate project management planning techniques and tools that support the project lifecycle.
	6.3 LO 3: Describe and evaluate concepts of IT baseline

	management for project planning and performance measurement. Describe the relationship of processes, such as Earned Value Management, operational analysis, and business performance measurement, to IT baseline management.
	6.3 LO 4: Identify and evaluate metrics to manage cost, schedule, and performance throughout the project lifecycle.
	6.3 LO 5: Using a business case and the federal Techstat model, analyze project performance, resource usage, and cost and schedule management. Discuss the potential tradeoffs required to balance competing drivers.
• OMB M-10-27 • OMB Guidance on Exhibit 300 • ANSI/EIA 748	6.3 LO 6: Discuss the required use of Earned Value Management by OMB to evaluate the performance of major federal IT investments.
	6.3 LO 7: Use an Earned Value Management System to analyze a business case.
	6.3 LO 8: Discuss the importance of program control processes and industry best practices.
	6.3 LO 9: Discuss the importance of financial management techniques and tools.
Competency 6.4 - Project quality management	6.4 LO 1: Define characteristics of quality; include usability, quality assurance and quality control. (See also Competency 3.4 on Quality improvement models and methods.)
	6.4 LO 2: Identify quality requirements and establish evaluation metrics to achieve those requirements.
	6.4 LO 3: Identify and discuss ways to build quality into systems.
	6.4 LO 4: Design and implement approaches to obtain feedback from users.
	6.4 LO 5: Discuss the advantages of independent verification and validation (IV&V) and design approaches to tie IV&V to the quality assurance program.
Competency 6.5 - Project risk management	6.5 LO 1: Define risk. (See also 7.2 LO 1.)
	6.5 LO 2: Define the risk management process.
• ISO 31000 series	6.5 LO 3: Discuss technical, cost, supply chain, and management capability risks associated with project management. (See also 7.3 LO 2.)
• DoD Acquisition Risk Management Guide, 6th Edition, Version 1.0	6.5 LO 4: Discuss the use of risk management tools, including a risk register.

• SEI at Carnegie Mellon University	
	6.5 LO 5: Demonstrate the ability to perform SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis.
	6.5 LO 6: Identify approaches to quantify risk assessment and to prioritize among risks.
	6.5 LO 7: Describe and evaluate the risk mitigation process, and how it is tailored to particular situations.
	6.5 LO 8: Evaluate monitoring and control systems and discuss their implementation.
	6.5 LO 9: Discuss the need for continuous risk monitoring throughout the project or program lifecycle.
	6.5 LO 10: Describe budget strategies to mitigate the impact of changes in project scope.
Competency 6.6 - System lifecycle management	6.6 LO 1: Discuss the IT lifecycle as a discipline. List and describe the components of the system lifecycle.
• SEI at Carnegie Mellon University • ISO/IEC 12207 • ISO 9000 series	6.6 LO 2: List and describe the standards that apply to the lifecycle.
	6.6 LO 3: Identify the impacts of costs, benefits, risks, resources, and time to market on the system lifecycle.
	6.6 LO 4: Distinguish between system development lifecycle and the system lifecycle.
	6.6 LO 5: Define and construct various project documents required throughout the system lifecycle and discuss how often they should be updated.
	6.6 LO 6: Describe the impact of Commercial-off-the-shelf (COTS) availability to the build or buy decision.
	6.6 LO 7: Discuss the heuristics of lifecycle—when to know when you have enough, etc. Include Total Cost of Ownership, lessons learned, etc.
	6.6 LO 8: Discuss the importance of managing change.
.	6.6 LO 9: Discuss the complexities associated with the closeout of systems, including end of life, the termination of systems, destruction of databases, etc.
	6.6 LO 10: Discuss strategies to increase investment effectiveness, such as agile, incremental development.

Competency 6.7 - Software development, testing, and implementation • ISO 9000 series • ISO/IEC 12207	6.7 LO 1: Evaluate the strengths and weaknesses of different models, approaches and methodologies relating to software development such as CMMI, Rapid Application Development (RAD), Joint Application Design (JAD), Object-Oriented (OO) software, Spiral Development, agile development, and emerging best practices. (See also Competency 12.6 on Software development technology.)
	6.7 LO 2: Discuss the importance of adopting and applying a systems engineering perspective and process to software development.
	6.7 LO 3: Develop an analytical process to support the make versus buy decision.
	6.7 LO 4: Discuss Pareto's 80/20 law as it applies to software development.
	6.7 LO 5: Discuss federal requirements for privacy, security, records management and accessibility in relation to software development. (See also 8.5 LO 5 and 9.2 LO 1.)
• ISO/IEC 9126	6.7 LO 6: Describe elements for evaluating software quality and how they would be applicable in testing software capabilities. (See also 8.5 LO 5.)
	6.7 LO 7: Discuss available tools, techniques, and metrics for software testing.
Competency 6.8 - Vendor management	6.8 LO 1: Discuss how to craft service level agreements which support mission and business objectives.
	6.8 LO 2: Discuss best practices for vendor selection criteria and processes.
	6.8 LO 3: Discuss how to establish useful vendor management policies and conformance criteria. (See also 2.4 LO 8.)
	6.8 LO 4: Discuss how to implement vendor management techniques that support long term business value and resource management.
	6.8 LO 5: Discuss the importance of vendor exit strategies in order to minimize disruption to IT services.
Competency 6.9 - IT program management leadership	6.9 LO 1: Discuss the characteristics of highly effective IT program managers.
	6.9 LO 2: Examine practices to influence and manage a broad set of stakeholder communities engaged in an IT program.
	6.9 LO 3: Examine ways IT leaders use methods of effective conflict management and negotiation.
	6.9 LO 4: Identify and discuss the steps required to

	successfully steward an integrated project team.
	6.9 LO 5: Design governance model processes for IT program management oversight and decision making.
	6.9 LO 6: Describe the role of vendors as strategic partners in IT programs.

7.0: Capital Planning and Investment Control (CPIC) • Title V, Acquisition Management, Federal Acquisition Streamlining Act of 1994, PL 103-355) • 31 U.S.C. Chapter 9 • Subtitle III, Title 40 U.S.C. • OMB Circular A-11 • OMB Circular A-94 • OMB Circular A-123 • OMB Circular A-127 • OMB Circular A-130 • OMB M-10-27 • OMB M-11-29 • NIST SP 800-65	*General Discussion: It is essential that CIOs understand the importance of Capital Planning and Investment Analysis. Capital planning is needed to provide a framework for running government with the same disciplines as private business. In addition to passage of the Clinger-Cohen Act (now codified in Title 40), there is an array of other legislation and fiscal guidance which are significant to effective Capital Planning and Investment Control.*
• Statutory Pay-As-You-Go Act of 2010	7.0 LO 1: Discuss the appropriation process and how politics (both local agendas and national issues) may affect the capital planning and investment control process.
• CMU/SEI-2002-TR-010, Software Acquisition Capability Maturity Model (SA-CMM)	7.0 LO 2: Schematize the entire IT lifecycle (using your agency or component's budgeting cycle or SEI's Software Acquisition Capability Maturity Model at Carnegie Mellon). Include both funding and retirement, and show how integral performance measures can support each phase of the cycle.
	7.0 LO 3: Discuss the importance of aligning capital planning with the agency mission.
	7.0 LO 4: Evaluate the roles that core mission, outsourcing and redesign play in CPIC.
Competency 7.1 - CPIC best practices	7.1 LO 1: Identify and evaluate current CPIC best practices.
	7.1 LO 2: Develop approaches to examine internal and external processes and practices and to develop appropriate benchmarks.
Competency 7.2 - Cost benefit, economic, and risk analysis • OMB Circular A-94 • OMB M-12-06 (or current memorandum on discount rates)	7.2 LO 1: Describe and interpret a variety of methodologies used in cost benefit, economic and risk analysis. (See also Competency 6.5 on Project risk management).
	7.2 LO 2: Prepare a set of cost benefit, economic and risk analysis methodologies that can provide common standards for use throughout a large organization. (See also 7.6 LO 4.)
	7.2 LO 3: Compare and contrast the implications of

	commonly used metrics such as ROI, NPV, Internal or Modified Internal Rate of Return (IRR, MIRR) etc. This comparison should address not only the outputs of the metrics, but also the assumptions upon which the metrics are based.
	7.2 LO 4: Identify and define processes to ensure the consistency of applied metrics across a range of projects under consideration in the capital planning process. (See also 7.8 LO 1.)
	7.2 LO 5: Analyze cost and economic data, assess its quality, and communicate its meaning to others.
	7.2 LO 6: Identify and evaluate qualitative approaches that can be used in risk analysis in addition to the more traditional quantitative methodologies.
	7.2 LO 7: Discuss the purpose for doing a risk-adjusted ROI as part of developing a solid business case for a major IT investment.
	7.2 LO 8: When presented with a business need, evaluate a variety of solutions that include, but are not limited to, IT-based solutions.
Competency 7.3 - Risk management models and methods • ISO 31000 series • NIST SP 800-37	7.3 LO 1: Discuss the reasons why risk analysis and risk management are vital. Include discussion of the role risk management plays and how the specifics relate to the organization and its mission.
	7.3 LO 2: Discuss and illustrate major areas of risk such as cost, schedule, performance, technical considerations (including obsolescence) and management capability. (See also 6.5 LO 3.)
	7.3 LO 3: Compare and contrast the commonly accepted standards, tools, and methods used in risk management.
• OMB Circular A-94 • OMB Guidance on Exhibit 300 • OMB M-12-06 (or current memorandum on discount rates)	7.3 LO 4: Evaluate and apply commonly used best practices risk management models.
	7.3 LO 5: Apply risk management models and methods to selected business cases.
	7.3 LO 6: Discuss the limitations of risk management models and areas of risk that may not be captured within a modeling scenario.

Competency 7.4 - Weighing benefits of alternative IT investments • OPM ECQ 3	7.4 LO 1: Develop an analysis and decision-making process to ensure that a CIO will evaluate all alternatives (and not only IT alternatives) for new requirements.
• OPM ECQ 3	7.4 LO 2: Compare and contrast the commonly accepted standards, tools, and methods available for evaluating benefits of alternative IT investments.
• OMB Circular A-11 • OMB Circular A-94 • OPM ECQ 3	7.4 LO 3: Compare and contrast the advantages of uniform IT investment assessment standards versus the value of flexibility in assessing alternative IT investments.
	7.4 LO 4: Identify and discuss examples of shared solutions between organizations to leverage investments.
• OMB Circular A-11 • OMB Circular A-94 • OPM ECQ 3	7.4 LO 5: Discuss the role of forecasting in cost-benefit analysis.
• OMB Circular A-94 • OPM ECQ 3	7.4 LO 6: Evaluate cost benefits of alternative IT-and non IT-solutions, and be able to support and justify the best alternative.
	7.4 LO 7: Identify the types of decision tools and criteria that are used within the development lifecycle to determine when a system has reached maturity.
Competency 7.5 - Capital investment analysis models and methods	7.5 LO 1: Compare, contrast and demonstrate the use of the various capital investment models and methods.
	7.5 LO 2: Analyze select IT capital investment business cases using appropriate analysis models.
	7.5 LO 3: Compare, contrast and demonstrate the use of the various investment assessment models and methods, including Balanced Scorecard, as well as discussion of federal TechStat reviews and IT Dashboard ratings of investments.
Competency 7.6 - Business case analysis	7.6 LO 1: Discuss the elements of a comprehensive business case analysis, including management, customers, and technical costs.
	7.6 LO 2: Using case studies, examine how business case analysis provides the means to evaluate the quantitative and qualitative aspects of competing investment opportunities.
	7.6 LO 3: Verify the validity of measurements used in developing/calculating investment metrics.
	7.6 LO 4: Compare and contrast the models and methods of business case analysis, both in government and in industry. (See also 7.2 LO 2.)

Competency 7.7 - Investment review process	7.7 LO 1: Discuss the need for an investment review process. Identify the types of information that are needed and discuss identities and roles of key decision-makers.
	7.7 LO 2: Identify the information and measurement tools that will be needed for the investment review process. Include "checkpoints" that may trigger additional information.
	7.7 LO 3: Discuss different approaches to the investment review process. Include approaches that are oriented to the culture of the specific organization (e.g., some organizations are detailed and quantitative, others are consensus-based), and how to select an appropriate approach based on organizational culture.
• OMB Circular A-11	7.7 LO 4: Describe the stages of an investment review process.
• OMB Guidance on Exhibit 300	7.7 LO 5: Describe the capital planning process in lifecycle terms. Include OMB Circular A-11 in the discussion.
Competency 7.8 - IT portfolio management • Subtitle III, Title 40 U.S.C. • OMB Circular A-130	7.8 LO 1: Discuss the steps required to move from assessment of individual IT capital investments to an integrated process for managing IT investments as portfolios. (See also 7.2 LO 4.)
	7.8 LO 2: Identify and discuss portfolio management categorization techniques.
	7.8 LO 3: Establish analysis criteria and a process to link portfolio objectives to an agency's vision, mission, goals, objectives and priorities.
	7.8 LO 4: Discuss strategies and methods to support portfolio tradeoff decision making.
• OMB M-12-10	7.8 LO 5: Examine how the process of balancing portfolios, by terminating or adding investments, effectively contributes to agency goal achievement.
• EO 13589 • OMB M-11-29 • OMB M-12-10	7.8 LO 6: Discuss Federal Government requirements and initiatives to eliminate waste and duplication within IT portfolios.

8.0: Acquisition • OMB M-11-29 • OMB 25 Point Plan • OMB, OFPP memo on Guidance for Specialized IT Acquisition Cadres	*General Discussion: Acquisition links technology investment to the business outcomes and results, as defined by the end consumer. Acquisition needs to move from what been a singular focus on process to one that considers both process and objectives. Acquisition anticipates what is needed before it is officially stated, and develops requirements that include the end users and must be linked to business outcomes.* *The CIO must understand the new dynamic, and understand lifecycle management. He/she must move from a risk-averse process to one of risk management, and create an innovative acquisition environment throughout the organization. The CIO should monitor changes in acquisition models and methods.* *Acquisition includes four stages–(1) Defining the business objective; (2) Requirements definition and approval; (3) Sourcing and (4) Post-Award management—which are each critical to a successful IT acquisition.*
	8.0 LO 1: Compare and contrast acquisition, contracting, and procurement.
	8.0 LO 2: Describe each phase of the acquisition lifecycle.
	8.0 LO 3: Describe the CIO's involvement in the early phases of acquisition management (i.e., concept exploration and development of requirements).
	8.0 LO 4: Discuss how to encourage ethical acquisition behavior for all involved in the acquisition process.
Competency 8.1 - Acquisition strategy	8.1 LO 1: Describe how the strategic plan, annual performance plan, enterprise architecture and capital planning process drive the acquisition strategy.
	8.1 LO 2: Demonstrate the development of an acquisition strategy. Include interpretation of internal and external environments, shared and cloud first strategies,the business, fiscal and political environments, awareness of A76 methodology, contracting strategy, and technological and environmental changes in the development of the acquisition strategy.
	8.1 LO 3: Identify and evaluate the range of alternatives to acquisition that should be explored in the pre-phase of the project. Include the roles of technology, reengineering, architecture, training, process improvement, procedure modification, elimination of functions, etc., in the listing of alternatives.
	8.1 LO 4: Discuss the differences between acquisition as a

	planned event and as a reactive event.
	8.1 LO 5: Illustrate the use of cost, schedule, technology, and performance goals in the planning and management of acquisitions.
	8.1 LO 6: Identify examples of issues that should be included in a project description and statement of work.
	8.1 LO 7: Identify the issues a project manager needs to address in a procurement management plan.
Competency 8.2 - Acquisition models and methodologies	8.2 LO 1: Compare, contrast, and evaluate various acquisition philosophies. Include, but do not limit the identification to: changing the operational process instead of purchasing; doing the work in house or outsourcing; outsourcing to one or to several contractors; intergovernmental outsourcing; unitary Requests for Proposal (RFP) or multiple awards; and the level at which the acquisition is managed.
	8.2 LO 2: Define the components typically included in an acquisition model. These components might include the relationship between government and supplier, internal relations, the motivation of the supplier, elements of sourcing, etc.
	8.2 LO 3: Discuss how to select an acquisition model that fits the organization's mission, needs, and culture.
	8.2 LO 4: Compare, contrast, and evaluate traditional and streamlined methodologies used for federal IT acquisition.
	8.2 LO 5: Discuss the acquisition implications from federal initiatives to increase inter-agency shared services.
	8.2 LO 6: Discuss the components of agile IT acquisition.
	8.2 LO 7: Using tools, methodologies and rules, evaluate the development acquisition model/plan for different acquisitions. Include the vehicle to be used (i.e., GSA schedule, unitary RFP or multiple awards).
Competency 8.3 - Post-award IT contract management	8.3 LO 1: List and describe post-award contract management methods and strategies that must be incorporated during the planning phase of the contract. Include methods of control, benchmarks, performance measurement, contract change management, termination strategies, and documentation of lessons learned.
	8.3 LO 2: Discuss the importance of pre-termination and termination decision points.
	8.3 LO 3: Discuss how to manage inter-agency partnering

	issues and relationships after a shared service contract has been awarded.
Competency 8.4 - IT acquisition best practices	8.4 LO 1: Discuss how to monitor and evaluate commercial and public sector IT acquisition best practices.
• OMB 25 Point Plan • OMB, OFPP memo on Guidance for Specialized IT Acquisition Cadres	8.4 LO 2: Discuss how to design, develop and use integrated program teams for IT acquisition.
.	8.4 LO 3: Discuss the utility of lease versus purchase analyses for IT acquisitions.
	8.4 LO 4: Discuss the utility of in-house versus out-sourced or shared IT services (e.g., "cloud," software as a service, and platform as a service).
	8.4 LO 5: Discuss the ramifications of Section 508 of the Rehabilitation Act on the acquisition of electronic and IT (E&IT) products and services. Include in the discussion web-based tools that help government purchasers determine and document Section 508 requirements that apply to a particular E&IT acquisition. (See also 9.2 LO 5.)
	8.4 LO 6: Discuss methods to ensure that the Contracting Officer's Representative (COR) or Contracting Officer's Technical Representative (COTR) receives the necessary support of the IT management team and identify best practices specific to the interface between the COTR and the contracting officer.
Competency 8.5 - Software acquisition management • OMB Circular A-11 • OMB Circular A-130 • SEI at Carnegie Mellon	8.5 LO 1: Discuss the elements to include in a well-defined agency policy for acquisition of software.
	8.5 LO 2: Discuss common causes of cost, schedule and performance problems associated with software procurement.
	8.5 LO 3: Apply requirements management and risk mitigation techniques associated with software acquisition.
	8.5 LO 4: Discuss software acquisition models and tools used to manage lifecycle planning.
	8.5 LO 5: Evaluate software performance measures and metrics. (See also 6.7 LO 5 and LO 6.)

	8.5 LO 6: Discuss the total cost of software acquisition, including license ownership and renewal.
Competency 8.6 - Supply chain risk management in acquisition	8.6 LO 1: Identify and define the different supply chain issues (including people, data, and suppliers) and their associated risks, including commodity IT.
	8.6 LO 2: Evaluate a supply chain model to ensure its service delivery is mission-focused, optimized, and mitigates risk.
	8.6 LO 3: Explore optional expansion of potential supply chains through federal exchanges and auctions.

9.0: Information and Knowledge Management	*General Discussion: Under Title 40, Subtitle III, Chapter 113, Section 11315, Agency CIOs have information resources management (IRM) identified as their primary responsibility. Per Circular A-130, IRM encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology. As part of their information management responsibilities, the CIO must also deal with Privacy issues; Freedom of Information Act (FOIA) requirements; Open Government mandates; and accessibility issues, as well as the preservation of records to comply with business, operating, regulatory and legal requirements. In addition, the CIO may support knowledge management activities to preserve and share subject matter expertise.*
Competency 9.1 - Privacy, personally identifiable, and protected health information	9.1 LO 1: Explain generally accepted definitions of privacy and security. Distinguish between privacy issues and security concerns.
• 5 U.S.C. 552 and 552a • Health Insurance Portability and Accountability Act (HIPAA) of 1996 • E-Government Act • OMB Circular A-130 • OMB M-99-18 • OMB M-01-05 • OMB M-03-22 • OMB M-06-15 • OMB M-06-16 • OMB M-06-19 • OMB M-07-16 • OMB M-10-23 • OMB M-11-02 • NIST SP 800-122	9.1 LO 2: Identify and discuss legislation, regulations and policies regarding privacy, personally identifiable information, and protected health information.
	9.1 LO 3: Evaluate security and privacy laws and regulations, including FOIA, relative to transparency and open government.
	9.1 LO 4: Assess internal and external factors affecting an organization's privacy policies and practices. Include discussion of challenges presented with social networking capabilities and social engineering techniques.
	9.1 LO 5: Discuss and give examples of the importance of planning, developing, and implementing, maintaining, and disposing of systems which address privacy. (See also 12.4 LO 3.)

• E-Government Act • OMB Circular A-11 • OMB Circular A-130	9.1 LO 6: Explain the Privacy Impact Assessment (PIA) process, the type of events which require a PIA, and the content of a PIA.
	9.1 LO 7: Identify and discuss privacy issues that may occur relative to other IT responsibilities such as records management, archival records, FOIA requests, declassification, firewalls, and security involving partners (extended enterprises).
	9.1 LO 8: Discuss the importance of encrypting data at rest and in transit with respect to personal privacy and social engineering attacks and exploits.
Competency 9.2 - Information accessibility • 29 U.S.C. 794d (Section 508 of the Rehabilitation Act of 1973, as amended) • U.S. Access Board Standards • Federal Acquisition Regulation (FAR), Part 10.000-10.002 • Federal Enterprise Architecture (FEA: Security and Privacy Profile • OMB memorandum of July 19, 2010, Improving the Accessibility of Government Information	9.2 LO 1: List and discuss the laws, standards and regulations relative to accessibility. (See also 4.2 LO 5, 6.7 LO 5.)
	9.2 LO 2: Describe electronic and information technology (E&IT) to which U.S. Code title 29, section 794d requirements apply and identify which E&IT are exempt from the law.
	9.2 LO 3: Describe the benefits, attributes and application of different types of adaptive technologies.
	9.2 LO 4: Discuss individual agency and designated federal roles and responsibilities (e.g., OMB, GSA, and Department of Justice) in implementing Section 508 requirements.
	9.2 LO 5: Discuss how the CIO can advocate for E&IT accessibility in all phases of web technology and software development planning, development and procurement. (See also 8.4 LO 5, 9.6 LO 11.)

Competency 9.3 - Records and information management	9.3 LO 1: Describe the full lifecycle of information management from creation or acquisition through its final disposition. This includes organizing, categorizing, classifying, disseminating, and migrating information.
• 44 U.S.C. Chapter 31 • 5 U.S.C. §552 and 552a • E-Government Act • OMB Circular A-130 • OMB M-12-18 • National Archives and Records Administration (NARA) regulations • ARMA International Standards and Best Practices for Excellence in Managing Records and Information • ISO 15489-1	9.3 LO 2: Discuss records management requirements established in statute and regulation.
• 5 U.S.C. §552 and 552a • OMB M-12-18	9.3 LO 3: Identify and discuss the impact of information and records management requirements on systems design.
	9.3 LO 4: Discuss the role of records management in developing and maintaining information resources that support business needs and processes.
	9.3 LO 5: Discuss how records and information management support the integrity, authenticity, preservation of electronic records. Include discussion of information assurance, privacy implications, and FOIA compliance.
	9.3 LO 6: Identify and analyze records management strategies that contribute to cost-effective, productive information services.
	9.3 LO 7: Identify records management issues associated with vital records and disaster recovery and how to address those issues in your agency.
	9.3 LO 8: Compare, contrast and evaluate knowledge management and records management tools.
	9.3 LO 9: Identify IT applications to accelerate electronic record keeping in agencies.
	9.3 LO 10: Discuss the e-discovery phase of civil/criminal litigation and CIOs' responsibilities for records retention and preservation.

Competency 9.4 - Knowledge management	*General Discussion: Knowledge Management (KM) involves the use of disciplined processes (and their supporting tools) to optimize application of knowledge in support of the organization's overall mission. KM involves linking people to people, people to content and content to content.*
	9.4 LO 1: Define Knowledge Management and discuss how it may be used to support the strategic goals of an organization.
	9.4 LO 2: Explain how KM can improve individual and organizational effectiveness.
	9.4 LO 3: Identify ways to develop a culture of knowledge sharing, collaboration and support of KM.
	9.4 LO 4: Identify and evaluate technological tools that may be used in implementing KM systems.
	9.4 LO 5: Evaluate approaches to measuring the effectiveness of KM efforts.
	9.4 LO 6: Compare the various roles that a CIO may assume in support of Knowledge Management.
	9.4 LO 7: Formulate a KM process that incorporates best practices.
Competency 9.5 - Social media	9.5 L0 1: Discuss the pros and cons of allowing the open use of social media in federal agencies.
	9.5 LO 2: Describe how social media is changing the way collaboration occurs in agencies.
	9.5 LO 3: Describe how crowdsourcing impacts "silos" in federal agencies.
	9.5 LO 4: Describe how the "personal you" and the "official you" should operate in the federal and private social media spaces.
	9.5 LO 5: Discuss the elements that should be included in an agency social media policy.
Competency 9.6 - Web development and maintenance strategy	9.6 LO 1: Explore the organizational implications and structure needed for web-based development.
• E-Government Act • Digital Millennium Copyright Act • OMB M-11-15	9.6 LO 2: Discuss approaches to web content management.
	9.6 LO 3: Compare and contrast agency web governance models.
	9.6 LO 4: Discuss the importance of maintaining a disciplined process for software configuration changes to web sites.

	(See also 6.1 LO 7.)
• OMB M-05-04 • OMB M-11-24 • OMB Memorandum of April, 7, 2010 on Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act • Digital Government: Building a 21st Century Platform to Better Serve the American People	9.6 LO 5: Identify legislative and policy requirements for government web-based development.
• OMB M-10-23	9.6 LO 6: Evaluate build/buy partnership issues relative to web development.
• OMB M-10-22	9.6 LO 7: Discuss the use of web analytics in business decision making and customer/client satisfaction.
• OMB Memorandum of September 28, 2010 on Transition to IPV6	9.6 LO 8: Compare, contrast and evaluate a single agency approach to web services delivery versus a multi-agency portal with a common infrastructure.
	9.6 LO 9: Assess the impact of web development technologies on government shared services. (Also see Competency 12.4 on Web technology.)
	9.6 LO 10: Discuss the challenges of “apps” development and deployment within the Federal Government, including the use of application programming interfaces (API) to share information.
	9.6 LO 11: Analyze considerations related to privacy, security and accessibility in government web development. (See also 9.2 LO 1, 10.4 LO 4, and 12.4 LO 3.)

Competency 9.7 - Open government • President's Memorandum on Transparency and Open Government • President's Memorandum on Building a 21st Century Digital Government • Digital Government: Building a 21st Century Platform to Better Serve the American People • OMB M-10-06	9.7 LO 1: Discuss the drivers influencing digital government at the federal level.
	9.7 LO 2: Compare and contrast the nature of government-based public information transactions and those that occur in private industry.
• Digital Government: Building a 21st Century Platform to Better Serve the American People	9.7 LO 3: Discuss the role of federal CIOs in open government.
	9.7 LO 4: Discuss the pros and cons of how open government impacts accountability for public officials and government performance.
	9.7 LO 5: Discuss the impact of public engagement on regulation and regulatory review.
	9.7 LO 6: Assess best practices and metrics available to measure public participation in open government.
	9.7 LO 7: Discuss available technologies to improve efficiency and access to government information.
	9.7 LO 8: Discuss the challenges agencies may encounter in providing digital services.
	9.7 LO 9: Analyze potential security concerns associated with open government.
	9.7 LO 10: Examine the impact of platforms such as data.gov and provide examples of their benefits.

Competency 9.8 - Information collection • 44 U.S.C. Chapter 35 • OMB Circular A-130 • OMB M-10-22 • OMB Memorandum of April 7, 2010 on Information Collection under the Paperwork Reduction Act	9.8 LO 1: Discuss the statutory and regulatory requirements associated with information collection both internally within an organization and externally from the public.
	9.8 LO 2: Discuss potential information collection and privacy issues associated with surveying individuals. Include in the discussion the data collection, storage and ownership implications that may occur based on who is conducting the survey (i.e., the agency, inter-governmental organization, private firm, contractor or other commercial entity).

10.0: Cybersecurity/Information Assurance (IA) • Subchapter III of Chapter 35 of Title 44, U.S.C. • International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World • Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure • National Strategy to Secure Cyberspace • OMB Circular A-130 • NSTISSI 4011 • CNSSI 4012 • CNSSI 4014 • ISO 27000	*General Discussion: The Federal Information Security Management Act (FISMA) – codified in Chapter 35 of Title 44, U.S. Code - charges each Federal CIO with the responsibilities to develop and maintain an agency-wide cybersecurity/information assurance(IA) program, including security policies, procedures and control techniques to both protect and defend information, systems and networks. CIOs must be able to assess the risks associated with vulnerable systems and information; determine the levels of security protection required; institute cost-effective methods to reduce risk to acceptable levels; and continuously monitor the capabilities of those techniques and controls. In addition, they must oversee the training programs to ensure that both the protectors and users of information and systems have the knowledge necessary to adequately protect organizational assets. The Office of Management and Budget (OMB) promulgates procedures for FISMA compliance and has levied additional requirements for cybersecurity/IA programs through OMB Circular A-130. Additionally, there are legislative and regulatory requirements that mandate specific care for certain types of information including (but not limited to) sensitive but unclassified information, corporate fiduciary information, personally identifiable information, and personal health information.*
	10.0 LO 1: Explain the enterprise cybersecurity/IA risks, national security risks, challenges, and opportunities associated with the current and future cybersecurity/IA environment.
	10.0 LO 2: Describe the operational and financial impacts of breaches in security and loss of trust on the business/mission of an organization.

Competency 10.1 - CIO Cybersecurity/IA roles and responsibilities • Subchapter III of Chapter 35 of Title 44, U.S.C. • OMB M-10-28 • OMB M-11-29 • CNSSI 4012 • NIST SP 800-100 • CMU/SEI-2005-TN-023, Governing for Information Security • ISO/IEC 27002 • Open Group, Information Security Management Maturity Model (ISM3)	10.1 LO 1: Analyze the Federal Information Security Management Act, codified in Subchapter III of Chapter 35 of title 44, U.S. Code, and related implementing guidance, (including National Institute of Standards and Technology (NIST), Office Management and Budget (OMB), and Committee on National Security Systems (CNSS) criteria) to determine the cybersecurity/IA roles and responsibilities of senior managers responsible for information or information systems/technology.
• NIST SP 800-53A • NIST SP 800-100	10.1 LO 2: Identify recognized sources of cybersecurity/IA best practices to include computer emergency readiness teams (e.g., US-CERT, U.S. Cyber Command, SEI's CERT Coordination Center); standards, configurations, and methodologies bodies (e.g., NIST Special Publications, ISO standards, common criteria); public/private partnerships (e.g., Center for Internet Security(CIS)); federal auditing agencies, e.g., GAO; federal regulatory or coordination bodies, e.g., Federal Energy Regulatory Commission (FERC), National Infrastructure Coordination Center (NICC); and commercial security institutes.
	10.1 LO 3: Define the items that constitute basic cybersecurity/IA literacy necessary to be a senior manager responsible for information or information systems/technology.
	10.1 LO 4: Identify and evaluate resources needed to achieve an acceptable level of security and to remedy security risk deficiencies based on system criticality and information sensitivity.

Competency 10.2 - Cybersecurity/IA legislation, policies, and procedures • Chapter 35 of Title 44, U.S.C. • Section 209 of the E-Government Act • Chapter 9 of Title 31, U.S.C. • Health Insurance Portability and Accountability Act (HIPAA) of 1996 • NIST FIPS and Special Publications Series • CNSS Issuances • ICD 503 • NSD-42 • GAO-09-232G • OMB M-07-11 • OMB M-07-18 • National Initiative for Cybersecurity Education	10.2 LO 1: Explain the important implications from the array of legislation, regulations and standards related to cybersecurity and information assurance (IA).
• OMB M-06-16	10.2 LO 2: Discuss how to evaluate security management policies and practices to ensure that they are cost effective and effectively reduce risk.
	10.2 LO 3: Describe how to apply cybersecurity/IA concepts to ensure compliance with other applicable requirements, including those standards and guidelines for national security systems issued in accordance with law and as directed by the President.
• NIST SP 800-53	10.2 LO 4: Develop and describe how to implement a methodology to annually evaluate the effectiveness of cybersecurity/IA policies, procedures, and practices.
	10.2 LO 5: Demonstrate how cybersecurity/IA is addressed throughout the lifecycle of an agency's information system.
• • NIST SP 800-61 • ISO/IEC 27002 • ISO/PAS 22399 • ITIL, Incident Management Open Guide • CMU/SEI-2007-TR-008	10.2 LO 6: Evaluate procedures for detecting, reporting, and responding to security incidents, to ensure that they are consistent with standards and guidelines issued pursuant to 44 U.S.C. 3546(b).
Competency 10.3 - Cybersecurity/IA Strategies and Plans	10.3 LO 1: Using a business case, evaluate the IA strategy for a major or critical IT system.
	10.3 LO 2: Evaluate the potential return on investment from technical countermeasures employed to meet security

	requirements.
	10.3 LO 3: Within an enterprise architectural framework, identify interdependency relationships and the associated impact resulting from cybersecurity/IA breach or compromise.
	10.3 LO 4: Discuss the need for procedural cybersecurity/IA safeguards during an IT acquisition process.
Competency 10.4 - Information and information systems threats and vulnerabilities analysis • CNSSI 4014	10.4 LO 1: Explain the use of the operations security (OPSEC) cycle (identifying critical information, analyzing threats, analyzing vulnerabilities, assessing risk, and applying countermeasures) for implementing a security system that protects information about a mission, operations or activity (thus denying or mitigating an adversary's ability to compromise or interrupt that mission, operation or activity).
• 6 U.S.C. 485 • CNSSI 4014	10.4 LO 2: Examine the inherent security challenges associated with implementing cross-agency information sharing capabilities. (See also 1.5 LO 2.)
• CNSSI 4014	10.4 LO 3: Analyze the security implications of software and hardware assurance, as it applies to confidentiality, and integrity, including legislation dealing with source manufacturing. Include internal GOTS, external COTS, internet/intranet, legacy codes, applicable legislation regarding source manufacturing, and the types of individuals (U.S. trained, foreign national H-1B visa holders, off-shore workforce, etc.) developing software.
	10.4 LO 4: Explain security issues and interdependencies related to various technologies and their impact on the security architecture of an organization. (See also 9.6 LO 11.)
• NSPD-54/HSPD-23 • OMB M-11-06 • NIST SP 800-42 • NSA Security Configuration Guides • DISA STIGs • http://sectools.org	10.4 LO 5: Formulate strategies to defend against the actions of state-sponsored attackers, hackers, hactivists, organized crime, industrial and international cyber espionage, advanced persistent threats, supply chain, and insider cyber threats.
	10.4 LO 6: Explain the role of human factors in cybersecurity/IA. Include human computer interaction, design, training, sabotage, human error prevention and error identification, personal use policies and monitoring, and internal contractor integrity.
• NIST SP 800-137	10.4 LO 7: Discuss how to develop and implement continuous monitoring practices.
• OMB M-06-16	10.4 LO 8: Explain the challenges and requirements

	associated with both logical and physical security of mobile and remotely-accessed information.
• NIST SP 800-37	10.4 LO 9: Evaluate security considerations and risks associated with emerging technology.
• NIST SP 800-37 • NIST SP 800-53	10.4 LO 10: Discuss how to address cybersecurity/IA requirements during technology transitions.
	10.4 LO 11: List and discuss available computer incident response assistance. Include US-CERT, Department of Energy's Computer Incident Response Capability, the U.S. Secret Service's National Threat Assessment Center, U.S. Cyber Command, the CERT Coordination Center and commercial services including MS Security Group and Cisco.
• OMB M-07-16	10.4 LO 12: Discuss breach notification requirements and how to effectively implement supportive agency procedures.
• OMB Federal Cloud Computing Strategy • NIST SP 500-291 • NIST SP 800-146 • GAO-10-513 • NSA, Cloud Computing – Overview of Information Assurance Concerns and Opportunities • Cloud Security Alliance for Critical Areas in Cloud Computing • GSA, Cloud IT Services	10.4 LO 13: Understand and evaluate the operational and financial benefits/tradeoffs of emerging technologies, and associated cybersecurity/IA benefits/tradeoffs, with respect to the use of virtualization capabilities, and cloud capabilities that deliver software, platform, or infrastructure as a service. (See also 12.7 LO 5.)
• OMB Federal Cloud Computing Strategy	10.4 LO 14: Discuss the security considerations of, and best practices for, "cloud" services (e.g., NIST, Cloud Security Alliance, ENISA, and Open Group's Jericho Forum). (See also 12.7 LO 5.)
• Federal Risk and Authorization Management Program (FedRAMP)	10.4 LO 15: Discuss the assessment and authorization (A&A) process related to cloud computing services and products. (See also 12.7 LO 5.)
	10.4 LO 16: Discuss the security requirements and risks associated with using service oriented architectures.

Competency 10.5 - Information security controls planning and management • Chapter 35 of Title 44, U.S.C. • 40 U.S.C. 11331 • NIST SP 800-53 (and associated publications) • FIPS PUB 199 • FIPS PUB 200 • CNSSI 4012 • CNSSI 4014 • OMB Circular A-130	10.5 LO 1: Determine the levels of cybersecurity/IA appropriate to protect an organization's information, information systems, and networks in accordance with standards promulgated under 40 U.S.C. 11331.
	10.5 LO 2: Explain the concepts of confidentiality, integrity, and availability as applied to Information Systems Security.
• CNSSI 4014	10.5 LO 3: Explain the use and types of security controls as directed in federal policies and procedures.
• CNSSI 4012	10.5 LO 4: Based on a risk analysis, select the security controls or other means to mitigate risks from unauthorized access, use, denial of service, disruption, modification, or destruction of information and information systems.
	10.5 LO 5: Develop a security plan and evaluate its compliance with agency and federal regulations for protection of the confidentiality, integrity, and availability of information, information systems, and networks. Discuss how to continually update the plan to incorporate lessons learned from prior incidents, address emerging technologies, and reflect evolving best practices.
• National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy • HSPD-12 • OMB M-11-11	10.5 LO 6: Explain the standards for employer and contractor identification prior to gaining physical access to federally controlled facilities and logical access to federally controlled information systems.
	10.5 LO 7: Describe how to evaluate the performance of security controls and techniques to ensure that they are effectively implemented (includes testing those security controls and techniques). Discuss current federal-wide initiatives.

Competency 10.6 - Cybersecurity/IA risk management • Chapter 35 of Title 44, U.S.C. • OMB Circular A-130, Appendix III • NIST SP 800-30 • NIST SP 800-37 • NIST SP 800-39 • NIST SP 800-53 • NIST SP 800-59 • CNSSI 4012 • ISO/IEC 27005	10.6 LO 1: Assess the risk and magnitude of the operational and financial harm that could result from the unauthorized access, use, disclosure, disruption, modification, denial of service, or destruction of agency information and information systems.

• NIST SP 800-37 • NIST SP 800-53	10.6 LO 2: Specify responsibilities and criteria for granting approvals.
• NIST SP 800-37 • NIST SP 800-53	10.6 LO 3: Develop implementing procedures for granting authority to operate (i.e., certification and accreditation).
• NIST SP 800-37 • NIST SP 800-53	10.6 LO 4: Formulate risk management plans to mitigate identified cybersecurity/IA weaknesses.
Competency 10.7 - Enterprise-wide cybersecurity/IA program management • Chapter 35 of Title 44, U.S.C. • OMB Circular A-130, Appendix III • NIST SP 800-100	10.7 LO 1: Evaluate an agency-wide cybersecurity/IA program and modify the program to comply with changes in policies, laws, regulations, standards, threats, and vulnerabilities.
	10.7 LO 2: Model how to document remedial action to address deficiencies in the cybersecurity/IA policies, procedures, and practices of an organization.
• Chapter 35 of Title 44, U.S.C. • NIST SP 800-16 • NIST SP 800-50 • CNSSI 4012 • ISO/IEC 27002	10.7 LO 3: Develop a plan and implementing procedures for a comprehensive cybersecurity/IA education and training program that includes tiered levels of training (e.g., general managers, personnel with significant responsibilities for information security, and general agency awareness training), as well as continuous learning requirements.
Competency 10.8 - Information security reporting compliance • Chapter 35 of Title 44, U.S.C. • OMB M-12-20 (or latest FY guidance) • OMB Guidance on Exhibit 300	10.8 LO 1: Discuss OMB IT security reporting requirements and develop an example of such a report.
• OMB M-11-33 • OMB M-12-20 • NIST SP 800-137	10.8 LO 2: Discuss the Department of Homeland Security's agency requirements for continuous monitoring and reporting through Cyberscope. (See also 10.4 LO 7.)
	10.8 LO 3: Develop policies to identify and comply with intrusion reporting requirements.
	10.8 LO 4: Develop the security and privacy sections for a business case.

Competency 10.9 - Critical infrastructure protection and disaster recovery planning • Chapter 35 of Title 44, U.S.C. • HSPD-7 • HSPD-8 • NSPD-51/HSPD-20 • National Strategy for the Physical Protection of Critical Infrastructures and Key Assets • National Infrastructure Protection Plan (NIPP • DHS, National Response Framework • OMB Circular A-130, Appendix III	10.9 LO 1: Explain concerns regarding the protection and safeguarding of America's critical infrastructures, both governmental and commercial, including power, transportation, banking and telecommunications systems. Include in the discussion key homeland security laws and policies, global trade practices and other efforts to protect and maintain America's physical and cyber infrastructures.
	10.9 LO 2: Discuss the disaster recovery planning process and its place within the overall continuity of operations and business continuity management process. (See also Competency 4.4 on Contingency and continuity of operations planning (COOP.))
	10.9 LO 3: Discuss the major elements involved in disaster recovery planning ranging from dealing with the emergency situation to recovery.

11.0: Enterprise Architecture • Federal Enterprise Architecture (FEA) • FEA Framework (FEAF) • FEA Reference Model • GAO-10-846G	*General Discussion: An enterprise architecture (EA) establishes the agency-wide roadmap(s) to meet mission and strategic goals through the optimal performance of core business processes and supporting information resources (e.g. systems, applications, databases, websites, and networks). Enterprise architecture roadmaps are essential for transforming the existing business processes and IT solutions to an optimal business capability target that provides maximum mission value. EA includes agile plans for transitioning from the current business and technology operating environment to the target environment.*
	11.0 LO 1: Explain the multi-dimensional nature of how enterprise architecture describes and documents the existing and target enterprise, how architecture supports the organization's current and future mission, and why architectures must be agile in order to support changing conditions.
	11.0 LO 2: Describe business reasons for developing an enterprise architecture (EA) and discuss benefits that can be derived from successful implementation of a sound EA.
Competency 11.1 - Enterprise architecture functions and governance	11.1 LO 1: Identify and describe roles in an EA program, such as those for the Executive Sponsor, Chief Information Officer, Chief (or Enterprise) Architect, Solutions Architects, Data Architects, and Systems Architects.
	11.1 LO 2: Describe the symbiotic relationship between strategic planning and EA and their impacts on visionary planning, portfolio management, and IT governance.
• Subtitle III of Title 40, U.S.C. • Chapters 35 and 36 of Title 44, U.S.C. • E-Government Act • OMB Circular A-130 • OMB Circular A-11 • Federal Enterprise Architecture (FEA) • FEA Framework (FEAF) • FEA Reference Model • GAO-10-846G	11.1 LO 3: Describe and discuss impacts of key regulatory requirements and guidance as they relate to enterprise architecture.
	11.1 LO 4: Describe the role of the Federal Enterprise Architecture (FEA) and how it contributes to cross-agency architecture practices.

	11.1 LO 5: Discuss the role of the Federal CIO Council in influencing agency EA practices.
	11.1 LO 6: Identify the EA responsibilities of internal agency managerial boards and committees and how they contribute to the agency's business and technology governance processes.
	11.1 LO 7 Describe how EA governance and EA planning provide complementary roles and discuss the benefits of integrated governance and planning processes.
Competency 11.2 - Key enterprise architecture concepts	11.2 LO 1: Identify and describe the purpose of the main elements of an enterprise architecture, including drivers, analysis, strategic direction, baseline and agile targets, focused road maps, alignment to services, programs and portfolios, work products, standards and best practices.
	11.2 LO 2: Describe the major EA components and how they are used in decision making, prioritization and budgetary processes.
	11.2 LO 3: Describe the relationship between EA and emerging technologies and standards, as well as the use of accepted standards.
	11.2 LO 4: Compare and contrast the dimensions and benefits of different architectural frameworks.
• FEA • FEAF	11.2 LO 5: Describe the purpose and use of reference models in enterprise architecture development and how they bring value to the decision making, prioritization, and budgetary processes.
	11.2 LO 6: Describe how the FEA reference models and profiles can be used to support agency IT program analysis and annual status reporting.
	11.2 LO 7: Identify EA best practices for each level of the architecture and demonstrate how to apply them in practical ways to optimize IT portfolios, programs and services.
	11.2 LO 8: Discuss the need to integrate security and privacy requirements into the EA. Include issues such as cross-realm security, security consequences of aggregated architectural data, common identity management approaches, data loss prevention and revocation/repudiation mechanisms.

Competency 11.3 - Enterprise architecture interpretation, development, and maintenance • OMB, Improving Agency Performance Using Information and Information Technology (Enterprise Architecture Assessment Framework)	11.3 LO 1: Discuss how to assess an agency's baseline architecture in terms of its effectiveness in meeting enterprise/strategic goals and performance goals and identify gaps that should be addressed.
	11.3 LO 2: Describe basic architecture documentation (i.e., work product) methodologies at each level of a commonly used framework (e.g., Federal Enterprise Architecture Framework (FEAF), the Department of Defense Architecture Framework (DODAF), or the Zachman Framework).
	11.3 LO 3: Discuss the purpose and value of automated tools to document, analyze, and monitor the enterprise architecture.
	11.3 LO 4: Discuss the importance and key aspects of model interpretation in understanding and sharing metadata, integration and component reuse, and achieving interoperability.
	11.3 LO 5: Discuss the benefits and importance of understanding the history of an organization's architecture and the business cases that were used to support it.
	11.3 LO 6: Discuss the relationship between the strategic planning process and EA and how linking these disciplines improves IT portfolios and operations. (See also 5.1 LO 6.)
	11.3 LO 7: Compare, contrast and evaluate internal and external drivers for new and emerging technology and their business implications.

Competency 11.4 - Use of enterprise architecture in IT investment decision making	11.4 LO 1: Discuss the importance of mapping major IT capital investments to the organization's strategic goals and business line activities, as well as alignment with an agency's target architecture.
	11.4 LO 2: Discuss how to achieve buy-in from Line of Business owners and senior executives to maintain sufficient resources for an effective EA program.
	11.4 LO 3: Describe how to resolve competing architectural principles to ensure best practices are maintained and architectural analysis remains useful in the decision making process.
	11.4 LO 4: Describe how an integrated capital planning and EA process can improve mission performance in spite of continually changing IT and agency requirements.
• FEA • OMB Circular A-11 • OMB Circular A-130	11.4 LO 5: Describe the relationship between the practical implementation of Federal Enterprise Architecture Reference Models and an agency's capital planning and investment control process. Include a discussion of related sections of OMB Circulars A-11 and A-130.
Competency 11.5 - Enterprise data management	11.5 LO 1: Describe the basic components of a data management program.
	11.5 LO 2: Discuss the criticality of data interoperability and quality to enterprise-wide information exchange, and the role of data standardization in supporting interoperability.
	11.5 LO 3: Describe current federal information exchange standards that are used and their role in intra- and inter-governmental sharing of information.
	11.5 LO 4: Discuss how the data architecture can be used to prioritize the elements of a data management program.
	11.5 LO 5: Describe the attributes of data quality and how architectural practices can improve data quality and application development within an agency.
• FEA Consolidated Reference Model	11.5 LO 6: Compare and contrast the differences between data management and records management and how they may support one another.
Competency 11.6 - Performance measurement for enterprise architecture	11.6 LO 1: Define and describe performance goals and distinguish performance goals from performance standards.
• FEA Consolidated Reference Model	11.6 LO 2: Discuss and describe the role of IT performance goals and standards with respect to the enterprise/program strategic plan, general goals and performance goals.

	11.6 LO 3: Discuss how automated network, security, and application monitoring tools can be used for trend analysis and establishing performance indicators as part of a CIO's "dashboard." (See also 5.3 LO 2, 5.5 LO 3, and 5.6 LO 1.)

12.0: Technology Management and Assessment • OPM ECQ 4	*General Discussion: Since the inception of the Clinger-Cohen Act, the CIO's role as technology manager has become increasingly complex. The ability to ensure effective development and deployment of technology requires a broad awareness of current and emerging technology capabilities, standards, policies and law. CIOs must also be able to identify and evaluate the strategic benefits of technology applications within the business environment.*
Competency 12.1 - Network, telecommunications, and mobile device technology	12.1 LO 1: Explain data transmission concepts, functions, and mechanisms.
	12.1 LO 2: Explain the capabilities and limitations of data transmission modes and media.
	12.1 LO 3: Evaluate the benefits and limitations of commonly-used local wired and wireless voice and data communication architectures, devices, and protocols.
• NIST SP 800-153	12.1 LO 4: Evaluate the benefits and limitations of commonly-used wide-area wired and wireless voice and data architectures, networks, devices and protocols.
• Digital Government: Building a 21st Century Platform to Better Serve the American People	12.1 LO 5: Describe how broader laws, policies and standards have been impacted by evolving mobile technology.
	12.1 LO 6: Discuss the processes and tools associated with developing, testing and distributing mobile applications.
	12.1 LO 7: Discuss the key elements required for effective mobile device management within an organization.
• Digital Government: Building a 21st Century Platform to Better Serve the American People • A Toolkit to Support Federal Agencies Implementing Bring Your Own Device Program	12.1 LO 8: Debate the pros and cons of implementing a "bring your own device" (BYOD) program.
Competency 12.2 - Spectrum management	12.2 LO 1: Define spectrum and evaluate the relationship between federal agency missions and spectrum management.
• FCC National Broadband Plan	12.2 LO 2: Assess the potential impacts on spectrum availability and management arising from increased domestic and international demand.
• FCC National Broadband Plan • NTIA Manual of Regulations and	12.2 LO 3: Identify and discuss federal and international laws and regulations that govern spectrum management.

Procedures for the Federal Radio Frequency Management	
	12.2 LO 4: Identify and evaluate tools and techniques available for effective spectrum management.
	12.2 LO 5: Identify recognized sources of best practices in spectrum-efficient technologies.
	12.2 LO 6: List and discuss spectrum management architecture issues and interdependencies.
	12.2 LO 7: Discuss supportability requirements that must be met prior to acquisition or modification of a new/existing telecommunications system.
Competency 12.3 - Computer systems	12.3 LO 1: Develop a plan for managing competing priorities among the portfolio of future hardware initiatives.
	12.3 LO 2: Investigate methods for managing hardware obsolescence.
	12.3 LO 3: Articulate a process for judging when to upgrade hardware based on emerging software requirements.
	12.3 LO 4: Demonstrate how to manage transitions from legacy systems.
	12.3 LO 5: Describe strategies to manage the changing integration among software.
Competency 12.4 - Web technology	12.4 LO 1: Review World Wide Web Consortium standards and discuss how they impact web technology development.
	12.4 LO 2: Define Extensible Markup Language (XML) standards and use. Relate the XML standards to the Federal Enterprise Architecture (FEA) Data Reference Model (DRM).
• OMB M-10-22	12.4 LO 3: Discuss the impact of web technology on privacy. (See also 9.1 LO 5 and 9.6 LO 11.)
	12.4 LO 4: Define and evaluate the use of Service Oriented Architectures (SOA) as they relate to web technology development. Relate SOA to the Federal Enterprise Architecture (FEA) Service Component Reference Model (SRM).
	12.4 LO 5: Define and evaluate industry best practices related to development and maintenance of SOA services.
	12.4 LO 6: Explain how performance metrics are used to measure the effectiveness of web technology development and deployment.
	12.4 LO 7: Discuss the challenges and opportunities associated with integrating new technologies and

	applications into the Federal Government's IT infrastructure.
Competency 12.5 - Data management technology	12.5 LO 1: Discuss the evolution of database management systems and the implications of various structural approaches.
	12.5 LO 2: Discuss the complexities associated with big data.
	12.5 LO 3: Describe best practices associated with data warehouse management.
	12.5 LO 4: Outline the rationale behind data mining and describe the varied uses of data mining.
	12.5 LO 5: Describe the benefits and challenges of enterprise business intelligence.
	12.5 LO 6: Detail the roles of XML and Radio Frequency Identification (RFID) in data management.
	12.5 LO 7: Discuss Online Analytical Processing (OLAP) and the associated benefit of the use of multidimensional information.
Competency 12.6 - Software development technology	12.6 LO1: Discuss how SOA enables the development and use of new web services that can support integration and governance requirements.
	12.6 LO 2: Compare the benefits and limitations of open source software with vendor developed software.
	12.6 LO 3: Outline the criteria for determining whether to use COTS or other types of software. (See also Competency 6.7 on Software development, testing and implementation.)
	12.6 LO 4: Discuss the evolution of enterprise resource planning (ERP) and customer relationship management (CRM), as well as major ERP and CRM implementation challenges.
	12.6 LO 5: Describe the objectives of software assurance, and how best to incorporate them into an information technology organization.
	12.6 LO 6: Discuss software as a service, and outline the criteria for deciding to purchase software in this manner.
	12.6 LO 7: Discuss the range of applications made possible by geographic information systems.

Competency 12.7 - Cloud Computing • NIST SP 800-145 • NIST SP 800-146	12.7 LO 1: Define cloud computing, the general cloud environments, and service models.
• NIST SP 800-146	12.7 LO 2: Outline the criteria for deciding to use cloud computing services.
	12.7 LO 3: Discuss the challenges associated with implementing identity and access standards across the cloud.
• NIST SP 800-144	12.7 LO 4: Discuss privacy implications and develop principles for a privacy framework within the cloud.
• NIST SP 800-53 • NIST SP 800-144	12.7 LO 5: Evaluate information security considerations and risks associated with cloud computing. (See also 10.4 LO 13, 14, and 15.)
	12.7 LO 6: Discuss data management and reliability issues associated with cloud computing.
	12.7 LO 7: Discuss the challenges associated with cloud deployment and migration.
	12.7 LO 8: Discuss cloud reliability and continuity of operations.
• OMB Federal Cloud Computing Strategy	12.7 LO 9: Discuss public and private sector cloud computing initiatives.
Competency 12.8 - Special use technology	12.8 LO 1: Define, discuss and investigate the use of Supervisory Control and Data Acquisition Systems (SCADA) in government systems.
	12.8 LO 2: Define metrics to assess the effectiveness of SCADA systems used in contractor systems.
	12.8 LO 3: Discuss the use of collaborative technology within the Federal Government.
	12.8 LO 4: Define metrics to assess the effective use of collaborative technology at all government levels.
	12.8 LO 5: Investigate industry best practices using collaborative technology to support global management and data exchange.
	12.8 LO 6: Define, discuss and investigate the use of modeling and simulation technology.
	12.8 LO 7: Describe how gamification can be used to address various challenges faced by the Federal Government.

	12.8 LO 8: Define, discuss and evaluate Human Computer Interface (HCI) technology.
	12.8 LO 9: Define metrics to assess the effective use of HCI technology in government systems.
	12.8 LO 10: Discuss and evaluate the capabilities of biometric-based personal identification/verification technology.
	12.8 LO 11: Discuss and evaluate the capabilities of the most common forms of social media.
Competency 12.9 - Emerging technology	12.9 LO1: Evaluate internal and external information sources of information on new and emerging technologies and their business implications.
	12.9 LO 2: Discuss approaches to aligning agency regulations and policies with emerging technologies and behavioral trends.
	12.9 LO 3: Describe strategies for managing competing priorities among the portfolio of future hardware (and related software) initiatives.
	12.9 LO 4: Describe how disruptive technologies support innovation and their impact, both positive and negative, on the business marketplace.

Appendix A - List of References

American National Standards Institute (ANSI)	**American National Standards Institute/Project Management Institute (ANSI/PMI) 99-001-2008:** Guide to the Project Management Body of Knowledge (PMBOK Guide) **American National Standards Institute/Electronic Industries Alliance (ANSI/EIA)-748:** Earned Value Management Systems
Committee on National Security Systems Instruction (CNSSI)	**CNSSI 4012:** National Information Assurance Training Standard for Senior System Managers **CNSSI 4014**: National Information Assurance Training Standard for Information Systems Security Officers
Department of Homeland Security	National Infrastructure Protection Plan, 2009 National Response Framework, January 2008 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003
Federal Chief Information Officers Council	Federal CIO Council Charter A Toolkit to Support Federal Agencies Implementing Bring Your Own Device Programs, August 23, 2012
Federal Communications Commission (FCC)	National Broadband Plan
Federal Continuity Directive (FCD)	**FCD 1:** Federal Executive Branch National Continuity **FCD 2:** Federal Executive Branch Mission Essential Functions and Primary Mission Essential Functions
Federal Information Processing Standards (FIPS) Publication (PUB)	**FIPS PUB 199:** Standards for Security Categorization of Federal information and Information Systems **FIPS PUB 200:** Minimum Security Requirements for Federal Information and Information Systems
Government Accountability Office (GAO)	**GAO Investment Guide** **GAO-04-394G:** Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity **GAO-09-3SP:** GAO Cost Estimating and Assessment Guide **GAO-09-232G:** Federal Information Systems Controls Audit Manual (FISCAM) **GAO-10-513:** Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing **GAO-10-846G:** Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management
Homeland Security Presidential Directive (HSPD)	**HSPD-7:** Critical Infrastructure Identication, Prioritization and Protection **HSPD-8:** National Preparedness **HSPD-12:** Policy for a Common Identification Standard for Federal Employees and Contractors **NSPD-51/HSPD-20:** National Continuity Policy **NSPD-54/HSPD-23:** Comprehensive National Cybersecurity Initiative
International Organization for Standardization (ISO)	**ISO 9000 series:** Quality Management **ISO 9001:** Quality Management Systems

	ISO/IEC 9126: Software Engineering – Product Quality **ISO/IEC 12207:** Systems and Software Engineering – Software Lifecycle Processes **ISO 15489-1:** Information and Documentation: Records Management **ISO/PAS 22399:** Guideline for Incident Preparedness and Operational Continuity Management **ISO/IEC 27000:** Information Security Management Systems Family of Standards **ISO/IEC 27002:** Information Security: Code of Practice for Information Security Management **ISO/IEC 27005:** Information Technology -- Security Techniques -- Information Security Risk Management **ISO 31000:** Risk Management Family of Standards **ISO 38500:** Corporate Governance of Information Technology
Intelligence Community Directive (ICD)	**ICD 503:** Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation
National Communications System Directive (NCSD)	**NCSD 3-10:** Minimum Requirements for Continuity Communications Capabilities
National Institute of Standards and Technology (NIST) Special Publication (SP)	**NIST SP 500-291:** NIST Cloud Computing Standards Roadmap **NIST SP 800-30:** Risk Management Guide for Information Technology Systems **NIST SP 800-34:** Contingency Planning Guide for Federal Information Systems **NIST SP 800-37:** Information Security: Guide for Applying the Risk Management Framework to Federal Information Systems **NIST SP 800-39:** Managing Information Security Risk - Organization, Mission, and Information System View **NIST SP 800-42:** Guideline on Network Security Testing **NIST SP 800-53:** Recommended Security Controls for Federal Information Systems and Organizations **NIST SP 800-53A**: Information Security: Guide for Assessing the Security Controls in Federal Information Systems **NIST SP 800-59:** Guideline for Identifying an Information System as a National Security System **NIST SP 800-61:** Computer Security Incident Handling Guide **NIST SP 800-65:** Information Security: Integrating IT Security into the Capital Planning and Investment Control Process **NIST SP 800-100:** Information Security Handbook: A Guide for Managers **NIST SP 800-122:** Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) **NIST SP 800-125:** Guide to Security for Full Virtualization Technologies **NIST SP 800-128:** Guide for Security-Focused Configuration Management of Information Systems **NIST SP 800-137:** Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations **NIST SP 800-144:** Guidelines on Security and Privacy in Public Cloud Computing **NIST SP 800-145:** The NIST Definition of Cloud Computing **NIST SP 800-146:** Cloud Computing Synopsis and Recommendations **NIST SP 800-153:** Guidelines for Securing Wireless Local Area Networks
National Security Directive (NSD)	**NSD 42:** National Policy for the Security of National Security Telecommunications and Information Systems
Office of Management and Budget (OMB) Circulars	**Circular A-11:** Preparation, Submission, and Executive of the Federal Budget **Circular A-94:** Guidelines and Discount Rates for Benefit-Cost Analysis of Federal

	Programs **Circular A-123:** Management's Responsibility for Internal Control **Circular A-127:** Financial Management Systems **Circular A-130:** Management of Federal Information Resources **Circular A-135:** Management of Federal Advisory Committees
OMB Guidance	Enterprise Architecture Assessment Framework (EAAF) Federal Enterprise Architecture (FEA) Consolidated Reference Model FEA Practice Guidance, November 2007 OMB Guidance on Exhibit 53: Information Technology and E-Government OMB Guidance on Exhibit 300: Planning, Budgeting, Acquisition and Management of Information Technology Capital Assets
OMB Numbered Memoranda	**M-99-18:** Privacy Policies on Federal Web Sites **M-01-05:** Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy **M-03-22:** OMB Guidance for Implementing the Privacy Provisions of th E-Government Act of 2002 **M-05-04:** Policies for Federal Agency Public Websites **M-05-08:** Designation of Senior Agency Officials for Privacy **M-06-15:** Safeguarding Personally Identifiable Information (PII) **M-06-16:** Protection of Sensitive Agency Information **M-06-19:** Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments **M-07-11:** Implementation of Commonly Accepted Security Configurations for Windows Operating Systems **M-07-16:** Safeguarding Against and Responding to the Breach of Personally Identifiable Information **M-07-18:** Ensuring New Acquisitions Include Common Security Configurations **M-09-02:** Information Technology Management Structure and Governance Framework **M-09-12:** President's Memorandum on Transparency and Open Government – Interagency Collaboration **M-10-06:** Open Government Directive **M-10-22:** Guidance for Online Use of Web Measurement and Customization Technologies **M-10-23:** Guidance for Agency Use of Third-Party Websites and Applications **M-10-27:** Information Technology Investment Baseline Management Policy **M-10-28:** Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS) **M-11-02:** Sharing Data While Protecting Privacy **M-11-06:** WikiLeaks – Mishandling of Classified Material **M-11-11:** Continued Implementation of HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors **M-11-15:** Final Guidance on Implementing the Plain Writing Act of 2010 **M-11-17:** Delivering on the Accountable Government Initiative and Implementing the GPRA Modernization Act of 2010 **M-11-24:** Implementing Executive Order 13571 on Streamlining Service Delivery and Improving Customer Service **M-11-26:** New Fast Track Process for Collecting Service Delivery Feedback Under the Paperwork Reduction Act

	M-11-29: Chief Information Officer Authorities **M-12-06:** 2012 Discount Rates for OMB Circular No. A-94 **M-12-09:** President's Memorandum on Transparency and Open Government – Interagency Collaboration **M-12-10:** Implementing PortfolioStat **M-12-18:** Managing Government Records Directive **M-12-20:** FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
OMB Unnumbered Memoranda	**April 7, 2010:** Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act **April 7, 2010:** Information Collection under the Paperwork Reduction Act **July 19, 2010:** Improving the Accessibility of Government Information **September 28, 2010:** Transition to IPV6 **July 13, 2011:** Guidance for Specialized Information Technology Acquisition Cadres
OMB Reports/Strategies	**June 2009**: Improving Agency Performance Using Information and Information Technology (Enterprise Architecture Assessment Framework) **December 9, 2010:** 25 Point Implementation Plan to Reform Federal Information Technology Management **February 8, 2011:** Federal Cloud Computing Strategy
Office of Personnel Management (OPM) Executive Core Qualifications (ECQ)	**ECQ 1 – Leading Change:** This ECQ involves the ability to bring about strategic change, both within and outside the organization, to meet organizational goals. Inherent to this ECQ is the ability to establish an organizational vision and to implement it in a continuously changing environment. Included in this ECQ are the competencies of creativity and innovation, external awareness, flexibility, resilience, strategic thinking, and vision. **ECQ 2 – Leading People:** This ECQ involves the ability to lead people toward meeting the organization's vision, mission, and goals. Inherent to this ECQ is the ability to provide an inclusive workplace that fosters the development of others, facilitates cooperation and teamwork, and supports constructive resolution of conflicts. Included in this ECQ are the competencies of conflict management, leveraging diversity, developing others, and team building . **ECQ 3 – Results Driven:** This ECQ involves the ability to meet organizational goals and customer expectations. Inherent to this ECQ is the ability to make decisions that produce high-quality results by applying technical knowledge, analyzing problems, and calculating risks. Included in this ECQ are the competencies of accountability, customer service, decisiveness, entrepreneurship, problem solving, and technical credibility. **ECQ 4 – Business Acumen:** This ECQ involves the ability to manage human, financial, and information resources strategically. Included in this ECQ are the competencies of financial management, human capital management, and technology management. **ECQ 5 – Building Coalitions:** This ECQ involves the ability to build coalitions internally and with other Federal agencies, State and local governments, nonprofit and private sector organizations, foreign governments, or international organizations to achieve common goals. Included in this ECQ are the competencies of partnering, political savvy, and influencing/negotiating.

Presidential Executive Orders (EO)	**EO 13231:** Critical Infrastructure Protection in the Information Age **EO 13388:** Further Strengthening the Sharing of Terrorism Information to Protect Americans **EO 13526:** Classified National Security Information **EO 13556:** Controlled Unclassified Information **EO 13576:** Delivering an Efficient, Effective, and Accountable Government **EO 13589:** Promoting Efficient Spending
Presidential Memoranda	**January 21, 2009:** President Barack Obama, Memorandum on Transparency and Open Government **May 23, 2012:** President Barack Obama, Memorandum Building a 21st Century Digital Government
Presidential Policy Directives (PPD)	**PPD-1:** Organization of the National Security Council System
White House Strategies	Digital Government: Building a 21st Century Platform to Better Serve the American People, May 23, 2012 National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information Sharing, 2009 National Strategy for Trusted Identities in Cyberspace, April 2011
United States Code	**5 U.S.C. §552:** The Freedom of Information Act, as amended by Public Law No. 104-231, 110 Stat. 3048 **5 U.S.C. §552a:** Records Maintained on Individuals **6 U.S.C. §485:** Information Sharing **29 U.S.C. §794d**: Section 508 of the Rehabilitation Act of 1973, as amended **31 U.S.C. Chapter 9:** Chief Financial Officers Act of 1990 **40 U.S.C. Subtitle III:** Information Technology Management (includes codified Clinger-Cohen Act) **44 U.S.C. Chapter 31:** Records Management by Federal Agencies **44 U.S.C. Chapter 35:** Coordination of Federal Information Policy (includes codified Paperwork Reduction Act) **44 U.S.C. Chapter 36:** Management and Promotion of Electronic Government Services
Other Statutes	E-Government Act of 2002 Federal Advisory Committee Act Federal Acquisition Streamlining Act of 1994, (PL 103-355), Title V, Acquisition Management Government Performance and Results (GPRA) Modernization Act of 2010 Statutory Pay-As-You-Go Act of 2010 (Title I of Public Law 111-139)
Miscellaneous	ARMA International Standards and Best Practices for Excellence in Managing Information and Records Department of Defense Acquisition Risk Management Guide, 6th Edition, Version 1.0 Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG)

National Security Agency (NSA) Security Configuration Guides

National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for the Federal Radio Frequency Management

Regulations of National Archives and Records Administration (NARA) (see Subchapter B of 36 Code of Federal Regulations Chapter XII)

U.S. Intelligence Community, Information Sharing Policy