Federal Chief Information Officers Council

December 29, 2006

Executive Committee

Executive Chair
Clay Johnson

Director
Karen S. Evans

Vice Chair
David M. Wennergren

Best Practices Committee
Co-Chairs
George O. Strawn
W. Hord Tipton

Architecture and Infrastructure
Committee Co-Chairs
Charles Havekost
Lisa Schlosser

IT Workforce Committee
Co-Chairs
Janet L. Barnes
Ira L. Hobbs

Section 508 Liaison
Craig Luigart

Cyber Security Liaison
Vance Hitch

TO: Federal CIO Council Members
FROM: Co-Chairs, Federal CIO Council IT Workforce Committee

SUBJECT: 2006 Clinger-Cohen Core Competencies

We are pleased to present the 2006 Clinger-Cohen Core Competencies.   In the ten years since the passage of the Clinger-Cohen Act, and the inception of core competency requirements for the IT workforce, each subsequent review has broadened and deepened the baseline IT Management knowledge and skills required for a CIO's staff.   This year, competencies have been added for IT Portfolio Management, Records Management, Software Acquisition Management, Technology Management and Assessment, and Cross-Boundary Process Collaboration. In addition, we have enhanced the Information Security/Information Assurance competencies to reflect legislative requirements and information security standards, and increased emphasis on Earned Value Management, Privacy, and Information Sharing.

The review process was a collaborative effort among thirteen federal agencies, academic representatives from both the Department of Defense's Information Resources Management College and the CIO University Consortium, and private industry members from the Industry Advisory Council.   The 2006 Clinger-Cohen Core Competencies and their associated learning objectives will be used as the foundation for IT course and curricula development, as well as the development and consistent implementation of IT workforce policy initiatives across the Federal Government.   This biennial effort fulfills IT workforce management requirements set forth in both Section 11315 of Title 40 and Section 209 of the E-Government Act.

Janet L. Barnes   Ira L. Hobbs

2006 Clinger-Cohen Core Competencies

The Federal CIO Council promotes continuous learning and professional development for the IT workforce by ensuring the Clinger-Cohen Core Competencies and their associated learning objectives are updated every two years. These Competencies serve as a baseline to assist organizations in complying with Section 11315 (c) (3) of Title 40 (Clinger-Cohen Act) and Section 209 of the E-Government Act. Federal Chief Information Officers should ensure that the knowledge, skills and abilities represented in each competency are resident within their organization.   More detailed learning objectives are provided in the 2006 Clinger-Cohen Core Competencies Learning Objectives on the Chief Information Officers Council (CIOC) web site.

1.0 Policy and Organization

1.1 Department/Agency missions, organization, functions, policies, procedures
1.2 Governing laws and authorities
1.3 Federal government decision-making, policy-making process and budget formulation and
     execution process
1.4 Linkages and interrelationships among Agency heads and COO, CIO, CTO and CFO functions
1.5 Intergovernmental programs, policies, and processes
1.6 Records management
1.7 Knowledge management

2.0 Leadership/Management

2.1 Defining roles, skill sets, and responsibilities of Senior Officials, CIO staff, and stakeholders
2.2 Methods for building federal IT management and technical staff expertise
2.3 Competency testing - standards, certification, and performance assessment
2.4 Partnership/team-building techniques
2.5 Personnel performance management techniques
2.6 Practices that attract and retain qualified IT personnel

3.0 Process/Change Management

3.1 Techniques/models of organizational development and change
3.2 Techniques and models of process management and control
3.3 Modeling and simulation tools and methods
3.4 Quality improvement models and methods
3.5 Business process redesign/reengineering models and methods
3.6 Cross-boundary process collaboration

4.0 Information Resources Strategy and Planning

4.1 IRM baseline assessment analysis
4.2 Interdepartmental, inter-agency IT functional analysis
4.3 IT planning methodologies
4.4 Contingency and continuity of operations planning (COOP)
4.5 Monitoring and evaluation methods and techniques

5.0 IT Performance Assessment: Models and Methods

5.1 GPRA (Government Performance and Results Act) and IT: Measuring the business value of

IT-and customer satisfaction

5.2 Monitoring and measuring new system development

5.3 Measuring IT success

5.4 Processes and tools for creating, administering and analyzing survey questionnaires

5.5 Techniques for defining and selecting effective performance measures

5.6 Examples of and criteria for systems performance evaluation

5.7 Managing IT reviews and oversight processes

6.0 IT Project/Program Management

6.1 Project scope/requirements management

6.2 Project integration management

6.3 Project time/cost/ performance management

6.4 Project quality management

6.5 Project risk management

6.6 Project procurement management

6.7 System life cycle management

6.8 Software development, testing and implementation

7.0 Capital Planning and Investment Control (CPIC)

7.1 Best practices

7.2 Cost benefit, economic, and risk analysis

7.3 Risk management- models and methods

7.4 Weighing benefits of alternative IT investments

7.5 Intergovernmental projects--federal, state, and local

7.6 Capital investment analysis-models and methods

7.7 Business case analysis

7.8 Investment review process

7.9 IT portfolio management

8.0 Acquisition

8.1 Acquisition strategy

8.2 Acquisition models and methodologies, from traditional to streamlined

8.3 Post-award IT contract management

8.4 IT acquisition best practices

8.5 Software acquisition management

9.0 E-Government

9.1 Strategic business issues and changes associated with E-Government
9.2 Web development and maintenance strategies
9.3 Industry standards and practices for communications
9.4 Channel issues (supply chains)
9.5 Dynamic pricing
9.6 Consumer/citizen information services
9.7 Information Accessibility (including Section 508 compliance)

10.0 Information Security/Information Assurance (IA)

10.1 CIO information security roles and responsibilities
10.2 Information security/related legislation, policies and procedures
10.3 Privacy and personally identifiable information
10.4 Information and information systems threats and vulnerabilities
10.5 Information security controls planning and management
10.6 IA risk management
10.7 Enterprise-wide information security program management
10.8 Information security reporting compliance
10.9 Critical infrastructure protection and disaster recovery planning

11.0 Enterprise Architecture

11.1 Enterprise architecture functions and governance
11.2 Key enterprise architecture concepts
11.3 Enterprise architecture interpretation, development and maintenance
11.4 Use of enterprise architecture in IT investment decision making
11.5 Data management
11.6 Performance measurement for enterprise architecture

12.0 Technology Management and Assessment

12.1 Network and telecommunications technology
12.2 Spectrum management
12.3 Computer systems
12.4 Web technology
12.5 Data management technology
12.6 Software development technology
12.7 Special use technology
12.8 Emerging technology