Pension Benefit Guaranty Corporation

Directive

Subject: Information Technology Management

Directive Number: IM 05-07

Originator: OIT

ALICE MARONI

Digitally signed by ALICE MARONI
Date: 2020.09.30 08:45:44 -04'00'

Alice C. Maroni
Chief Management Officer

1. **PURPOSE:** The Pension Benefit Guaranty Corporation (PBGC) Information Technology Management Directive establishes the policy for managing the full life cycle of Information Technology (IT) at PBGC.

2. **EFFECTIVE DATE:** This Directive updates PBGC Directive IM 05-07 dated 04/17/2020. This Directive is effective on the date shown above.

3. **SCOPE:** This Directive applies to all PBGC Federal employees and contractors who are responsible for or involved in any aspect of acquiring, managing, and implementing IT at PBGC, regardless of funding source or resources.

4. **AUTHORITIES:**

   a. Clinger-Cohen Act of 1996, 40 U.S.C. § 1401 et seq. (2012).
   b. E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899 (2002).
   c. National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.
   d. Office of Management and Budget (OMB) Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (June 28, 2019).
   e. OMB Circular No. A-130, Revised, *Managing Information as a Strategic Resource* (July. 28, 2016).
   f. PBGC Directive FM 05-01, PBGC Financial Management Systems.
   g. PBGC Order FM 05-2, Account Classification Structure/Code Combinations.
   h. PBGC Directive GA 15-05, PBGC Corporate Planning Process.
   i. PBGC Directive IM 05-02, PBGC Information Security Policy.
   j. PBGC Directive IM 10-03, Protecting Sensitive Information.
   k. PBGC Directive IM 05-09, PBGC Privacy Program.

5. **BACKGROUND:** This Directive establishes the PBGC policies, roles, and responsibilities under the Federal authorities for all aspects of managing the full life cycle of IT. The Clinger Cohen Act, OMB Circulars A-130 and A-11, directly guide this Directive to reform and improve how PBGC acquires and manages IT resources. The IT Solutions Life Cycle Management Framework (ITSLCM) framework incorporates requirements from IT Strategic Plan, Enterprise Architecture (EA), IT Portfolio Management (ITPfM), Cybersecurity, and Privacy.

6. **DEFINITIONS:** This Directive defines critical IT terminology. Definitions for additional IT terminology used in this Directive are available in the Office of Information Technology Glossary of Terms (GOTs), Security, and Privacy Directives located on the PBGC Intranet:

   a. **IT.** Any service, equipment, or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of PBGC's data or information, wherever located. IT can be hosted on PBGC premises, Provisioned IT Services, or Internal Delivery Service using different Delivery Methods (see below for definitions)**.** For the definition of Information System, please refer to PBGC Directive IM-05-02.

   b. **IT Solution.** The practical application of IT (or a combination of technologies) to solve a business need, gap, or problem.

   c. **ITSLCM.** A framework designed to manage IT Programs and Projects through the identification, planning, implementation, maintenance, and disposition of IT. Details of the ITSLCM are available on PBGC's Intranet.

   d. **IT Portfolio/Program/Project.**
      (1) **IT Portfolio.** A collection of IT Programs and Chief Information Officer (CIO) Programs reported to OMB in the form of Agency IT Portfolio Summary which account for total IT spending.
      (2) **IT Program (Major or Non-Major).** The use of IT resources for a collection of IT Projects, to achieve efficient and effective business operations to meet PBGC's strategic goals, performance goals and priorities, and strategies. Programs may be "Major" or "Non-Major". "Major" IT Programs are required to submit a Major IT Business Case (OMB A-11, Major IT Business Case) to OMB.
      (3) **IT Project and Release.** A project is a temporary endeavor with defined start and end dates that contributes to the IT Program's measurable benefits. An IT project may be delivered in one or more releases using various development approaches enabling modular development.

   e. **IT Program Planning/Development, Modernization, Enhancement (DME)/ Steady State/Services**.
      (1) **IT Program Planning.** Activities that are required to clearly define and document the business problem (gaps to be closed, measurable outcomes, and executive agreement) and a clear sequenced roadmap for implementing solutions (Business Process engineering or streamlining,

alternatives for addressing the problem, IT Solutions and products, etc.). IT Program Planning includes qualitative and quantitative measures for assessing success of the Program, a list of projects associated with furthering the Program goals and measures, impacts to other programs, and products. There may be other activities associated with managing the full lifecycle of the Program.

(2) **DME.** Includes introducing new or modifying existing IT solutions to substantively improve capability or performance, address legislative or regulatory requirements, or meet changing business requirements. DME may occur at any time during a program's life cycle. DME costs include the total cost of ownership for hardware, software development and acquisition costs, commercial off-the-shelf acquisition costs, government labor costs, and contracted labor costs for planning, development, acquisition, system integration, and direct project management and overhead support.

(a) **Development.** Projects to create new IT solutions (automating manual processes where an IT solution does not exist).

(b) **Modernization.** Projects to replace existing IT solutions (replacing technology components, data migrating, decommissioning of legacy technology which could result in increased capability).

(c) **Enhancement.** Projects to revise an existing production system that adds new functionality to the end user that satisfies additional end-user requirements.

(3) **Steady State/Operations and Maintenance (O&M).** Operating and maintaining an IT solution in a production environment per the last set of approved requirements. O&M includes activities associated with operation (service desk, backups, or disaster recovery/Continuity of Operations Plan) and maintenance changes (patching, vendor-supported versions, and defect correction) needed to sustain the IT solution at the current capability and performance levels. It includes corrective hardware and software maintenance, voice and data communications maintenance and service, replacement of broken or obsolete IT equipment, and disposal of an IT solution.

(4) **Baseline/Re-Baseline.** The approved work breakdown structure, costs, schedule, and performance goals for a given program, as defined in OMB Memo M-10-27. A baseline is a starting point for measuring performance of an IT Program/Project. A re-baseline is approved adjustments to the existing baseline.

(5) **Provisioned IT Services.** An IT service that is (1) owned, operated, and provided by an outside vendor or external government organization (i.e., not managed, owned, operated, and provided by the procuring organization) and (2) consumed by the agency on an as-needed basis. Examples of Provisioned IT Service may include the purchase of E-Government (E-Gov) Line of Business from another Federal Agency, or

the purchase of Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) from a private service provider, or the purchase of shared services or cloud services. Provisioned IT Service excludes Software Licenses but includes both Intra and Inter Shared Services (Source: OMB IT Budget – Capital Planning Guidance). In PBGC, provisioned IT services are composed of Managed and Shared Services.

(a) **Managed Service.** An IT enabled business capability provided by a commercial organization and is delivered through cloud or non-cloud platforms.

(b) **Shared Service.** An IT enabled business capability provided by a Federal agency for consumption within or between Federal Agencies and is delivered through cloud or non-cloud platforms. (Source: OMB Federal Information Technology Shared Services Strategy, May 2012.)

(6) **Internal Hosting Service.** An IT service that is owned, operated, provided by, and provided for PBGC and may be delivered by cloud or non-cloud methods.

(7) **Delivery Method.** A deployment model by which an IT service is delivered to the consumers of the service. Below are two methods:

(a) **Cloud Computing.** A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics: on-demand self-service; resource pooling; broad network access; rapid elasticity; and measured service. (Source: *The NIST Definition of Cloud Computing*, NIST SP 800-145 September 2011)

(b) **Non-Cloud Computing.** A service delivery method that does not meet all the NIST five essential characteristics of cloud computing. While some NIST essential cloud characteristics may be present, it is not considered cloud computing.

7. **POLICY:** It is PBGC policy that all IT owned and operated by or on behalf of PBGC will adhere to this Directive. Provisions prescribed herein govern how IT is managed and has been developed in accordance with applicable laws and regulations.

a. **IT Products and Services Acquisitions.** The Information Technology Infrastructure Operations Department (ITIOD) is responsible for all PBGC IT hardware and software acquisitions. All PBGC IT hardware and software purchases must be coordinated with ITIOD regardless of who funds or maintains it. All IT acquisitions (products and services) will be part of the IT Portfolio prior to initiating the acquisition process. All IT products shall be approved in the Technical Reference Model (TRM) prior to use in PBGC. The results of product

analysis on all new IT products will be presented to the Technical Review Board (TRB) for review prior to "selection" in the acquisition process.

(1) Accountable or Responsible: All PBGC Employees and Contractors who are responsible for or involved in any aspect of acquiring, managing, and implementing IT at PBGC.
(2) Governed By: IT Portfolio Review Board (ITPRB).
(3) Supported By: IT Portfolio Manager; Chief Enterprise Architect (CEA).
(4) Non-Compliance: Recommend to Chief Information Officer (CIO) to disapprove requisition.

b. **IT Program Classification.** The ITPRB classifies IT programs as Major or Non-Major. Major IT Programs have a total budgeted cost greater than or equal to $10M per year or $20M over three years. IT Programs not meeting the threshold of Major IT Programs are considered Non-Major IT Programs.

(1) Accountable or Responsible: ITPRB.
(2) Governed By: CIO.
(3) Supported By: IT Portfolio Manager; CEA.
(4) Non-Compliance: Funding disapproval from OMB.

c. **IT Program Planning.** IT Program Planning will be completed prior to technology implementation. Planning activities include conducting Business Needs Analysis (BNA); Alternatives and Cost-Benefit Analysis; Acquisition Strategy; identifying alignment to PBGC and IT Strategic Plans; leveraging existing technologies, or shared services across the Federal government.

(1) Accountable or Responsible: IT and Business Program Managers
(2) Governed By: ITPRB.
(3) Supported By: CEA; Chief Information Security Officer (CISO).
(4) Non-Compliance: Recommend to Budget and Planning Integration Team (BPIT) not to fund or designate as lower priority for funding projects.

d. **Total Cost of Ownership.** All IT Programs will develop, manage, and report full IT life cycle costs regardless of funding sources. This includes costs associated with planning, DME, O&M, Managed Services, pilots or prototypes, impacts to other IT Programs (as negotiated), end of service life, Cybersecurity, and Privacy.

(1) Accountable or Responsible: IT and Business Program Managers.
(2) Governed By: ITPRB.
(3) Supported By: CISO; CEA; Impacted Programs.
(4) Non-Compliance: Recommend to BPIT for unplanned costs to be covered by sponsoring department's baseline budget.

e. **IT Program Oversight and Governance.** All IT Programs will follow the following 5-Tier model for managing Scope, Cost, Schedule, Risks, and Issues: Tier 1 – Project Management (IT and Business); Tier 2 – Program Management (IT and Business); Tier 3 – Steering/Oversight Committees (CIO and associated Chief Officer (CXO); Tier 4 – PBGC Governance Boards (GA-15-05, ITPRB, BPIT, EMC); and Tier 5 – OMB.

(1) Accountable or Responsible:
  (a) Tier 1 – IT and Business Program Managers.
  (b) Tier 2 – CIO and CXO (or delegate).
  (c) Tier 3 – CIO and CXO.
  (d) Tier 4 – Board Chairs.
  (e) Tier 5 – OMB.

(2) Governed By:
  (a) Tier 1 – ITPRD
  (b) Tier 2 – ITPRD
  (c) Tier 3 – ITPRD
  (d) Tier 4 –Chief Management Officer.
  (e) Tier 5 – OMB.

(3) Supported By: ITPRB Members.

(4) Non-Compliance: Recommend the CIO and the associated CXO correct, place on-hold, or terminate the project. Also, recommend to BPIT to prioritize funding as low priority.

f. **Program and Project Managers.** All IT Programs will have a CIO-assigned IT Program Manager and a CXO-assigned Business Program Manager who possess the skills and capacity to perform their roles as defined in section 9 of this Directive. All IT Projects will have IT and Business project managers who possess the skills and capacity to perform their roles as defined in section 9 of this Directive.

(1) Accountable or Responsible: Programs- CIO (or delegates); Projects- IT and Business Program Managers.
(2) Governed By: ITPRB.
(3) Supported By: Sponsoring Departments; Business Innovation Service. Department
(4) Non-Compliance: Recommend to the CXO to correct issues; Recommend to BPIT to prioritize funding as low priority.

g. **Baseline and Re-Baseline.** All IT Programs and Projects will establish baselines for performance, scope, cost, and schedule. All IT Programs and Projects will obtain approval to establish or revise a baseline. For IT programs, CIO and sponsoring CXO approval are required. For IT Projects, IT and Business Program Manager's approval with CIO and CXO concurrence are required.

(1) Accountable or Responsible: IT and Business Program Managers.
(2) Governed By: ITPRB.
(3) Supported By: IT and Business Program Managers.
(4) Non-Compliance: ITPRB recommends to the CIO and CXO to disapprove cost overruns.

h. **ITSLCM Compliance.** All IT programs will comply with PBGC's ITSLCM, including control gates, IT standards, and artifacts.

(1) Accountable or Responsible: All PBGC employees and contractors who are responsible for or involved in any aspect of acquiring, managing, and implementing Information Technology at PBGC.
(2) Governed By: Enterprise Governance Department (EGD).
(3) Supported By: IT and Business Program Managers.
(4) Non-Compliance: EGD recommends actions to 5-tier Oversight and Governance structure.

i. **ITPRB Reviews.** All IT Programs will provide data transparency for the ITPRB to conduct prioritization, control, and evaluation reviews.

(1) Accountable or Responsible: IT and Business Program Managers.
(2) Governed By: ITPRB.
(3) Supported By: IT Portfolio Manager.
(4) Non-Compliance: ITPRB recommends actions to 5-tier Oversight and Governance

j. **Privacy Compliance.** All privacy requirements will be complied with.

(1) Accountable or Responsible: All PBGC employees and contractors who are responsible for or involved in any aspects of acquiring, managing, and implementing Information Technology at PBGC.
(2) Governed By: Senior Agency Official for Privacy (SAOP) (Refer to PBGC Directive IM 05-09, *PBGC Privacy Program* and PBGC Directive IM 10-03, *Protecting Sensitive Information*).
(3) Supported By: CIO, CISO (Refer to the following PBGC Directives: IM 05-02, *PBGC Information Security Policy*, IM 05-09, *PBGC Privacy Program* and IM 10-03, *Protecting Sensitive Information*).
(4) Non-Compliance: SAOP recommends remedy.

8. **POLICY DEVIATION:** The CIO or delegate has the authority to approve policy deviations (except deviations from Privacy compliance). Policy deviation requests will be submitted by a Department Director or higher. Justification memorandum will include:

a. IT Program or IT Project requesting exemption.
b. Requirements needing exemption.
c. Risk associated with policy deviation and steps taken to reduce those risks.
d. Risk acceptance for risks incurred if exemption is granted.
e. Benefits to be realized by providing the exemption.
f. Temporary or permanent request; if temporary, plans/dates for achieving compliance.
g. Identification of other pertinent data for obtaining an exemption.

9. **ROLES AND RESPONSIBILITIES**: Note: See Directive IM 05-02, *PBGC Information Security Policy* for descriptions of Cybersecurity related roles and responsibilities. See PBGC Directive IM 05-09, *PBGC Privacy Program* and PBGC

Directive IM 10-03, *Protecting Sensitive Information* for descriptions of Privacy related roles and responsibilities.

a. **IT Governance:**

(1) **CIO.** The CIO is responsible for PBGC's use of IT to achieve mission, business, and operational goals, while setting the future direction of IT through CIO Programs' plans (IT Strategic Plan, EA plans, and IT Capital Plan). The CIO establishes PBGC's EA Program, ITPfM Program, and Cybersecurity Program in accordance with Federal guidelines and customized to PBGC. The CIO reviews IT related Federal mandates with the Office of General Counsel to determine applicability and establishes appropriate IT policies/directives, processes, procedures, standards, and IT governance boards. The CIO shares knowledge of the IT Portfolio performance to influence overall PBGC budget decisions.

(2) **ITIOD.** This department is responsible for coordinating and acquiring all PBGC IT hardware and software purchases, regardless of who funds or maintains it.

(3) **Business Owner/Sponsor (CXO).** A Program area Executive Management Committee (EMC) member who works in partnership with the CIO and is responsible for communicating business goals, objectives, priorities, requirements, audit findings, and performance metrics to the Program Managers. Demonstrates stewardship by working collaboratively on shared business objectives. Sponsors their IT program, assigns Business Program Managers, includes IT funding in their departmental budget requests, and commits business resources for executing their IT Program and Projects. Actively participates in Program Steering/Oversight Committee.

(4) **ITPRB.** This governance board, chaired by the CIO or designee, reviews IT Program proposals and develops recommendations using established criteria concerning viability, cost-effectiveness, and alignment with the PBGC strategic goals and IT strategic goals. These recommendations are intended to inform the BPIT and EMC in order to drive executive-level understanding and application of funding. The ITPRB functions as PBGC's ITPfM governance board and implements the requirements of IT Capital Planning and Investment Control processes for the agency. For more details, please reference Directive PBGC Directive GA 15-05, *PBGC Corporate Planning Process*, and the charter, membership composition, and other related materials available on the PBGC Intranet.

(5) **TRB.** This governance board, chaired by the CEA or designee, reviews technology proposals and architectural designs of IT solutions for compliance with established IT standards and technical feasibility. TRB is the approving authority of IT Standards and use of technology products in the TRM. For more details, reference the charter, membership composition, and other related materials available on the Intranet.

(6) **Steering/Oversight Committee.** Comprised of the CIO, CXO, and their leadership (Department Directors), this committee sets business and IT Program goals, measures, and targets in alignment with the PBGC Strategic Plan and PBGC's IT Strategic Plan. It is responsible for providing joint sustaining sponsorship on priorities, funding, human capital resources, integration with other EMC program areas, and ensuring IT funding requests are included in departmental budget requests. It prioritizes IT Projects within its Program and approves IT program/project baselines followed by oversight of planning and execution of IT programs. It is responsible for conducting regular CIO-CXO IT Program and Project reviews (at least quarterly) to ensure IT Programs and IT Projects are performing towards scope/targets (e.g., providing value to the corporation, cost, and schedule), addressing escalated risks and issues, and requesting Corrective Actions or terminating non-performing projects within their program. Serves as the final approval authority for all external IT related reporting of their IT Programs.

b. **Program and Project Management:**

(1) **IT Program Manager.** The IT Program Manager, with the Business Program Manager, has the delegated authority from the CIO for making IT-related decisions for the successful outcome of IT Programs. They are responsible for managing the full lifecycle of their IT Program, from planning, execution, monitoring and control, to close-out in compliance with all IT Directives, processes, and procedures. The IT Program Manager is responsible for managing IT program integration, scope, total lifecycle cost, time, quality, procurement, human resources (business and IT), communications, risks, and issues. Define and establish a sequence of IT Projects in alignment with the Enterprise Target Architecture (ETA), and provides results of Business Needs Analyses and Corporate Strategic Priorities. Develop IT Acquisition Strategy with approval from Contracting Officer (CO). Coordinate IT program impacts with other IT program stakeholders. Designate IT Project Managers and manages IT capacity involvement of IT resources.

(2) **Business Program Manager.** The Business Program Manager, with the IT Program Manager, has the delegated authority from the Business Owner/Sponsor for making business related decisions for the successful outcome of IT Programs. The Business Program Manager is responsible for leading the Business Needs Analysis (BNA) with EA and business process assessment/engineering/improvements to establish streamlined business processes. Leads Alternative Analysis and Cost-Benefit Analyses, ensures the IT Program Acquisition Strategy aligns with departmental budget submissions, and ensures the IT Program yields benefits identified in the IT Program Plan. Designates Business Project Managers, manages business capacity, and ensures appropriate level of involvement of business impacted resources. Coordinates IT Program

impacts with other business area program stakeholders and enables business-to-business integration. Leads organizational change management to ensure introduction of IT solutions are embraced by the user community

(3) **Chief Enterprise Architect (CEA).** The CEA carries out the CIO's architecture responsibilities under the Clinger Cohen Act of 1996, E-Government Act of 2002, and OMB Circular No. A-130, including the development and use of an ETA (contains the enterprise current and target states) and transition plan. Ensures Business Needs Analyses are planned and completed prior to implementation of DME Projects. The CEA works with IT program teams to guide compliance with EA Standards, TRM, and the ETA, and appoints Enterprise Architects to Integrated Project Teams to promote reusability of solutions.

(4) **IT Portfolio Manager.** The IT Portfolio Manager ensures the best mix of programs and projects are contributing to an efficient IT Portfolio. Conducts trend analyses of the IT Portfolio, performs "what if" scenarios, leads the ITPRB through IT Portfolio decisions, and, makes recommendations to other boards. Provides guidance to IT Programs on strengthening business cases and manages communication with OMB and other external entities.

(5) **IT Project Manager.** The IT Project Manager (may also function as the Product Manager), with the Business Project Manager, has the delegated authority from the IT Program Manager for the successful outcome of IT Projects from planning, execution, monitoring and control, to closeout, working under the guidance of the IT Program Manager. The IT Project Manager is responsible for managing project integration, scope, cost, time, quality, procurement, human resources (business and IT), communications, risks, and issues. Coordinates IT project impacts with other project stakeholders and solutions.

(6) **Business Project Manager.** The Business Project Manager, (may also function as the Product Owner) with the IT Project Manager, has the delegated authority from the Business Program Manager for the successful outcome of IT Projects from planning, execution, monitoring and control, to closeout, working under the guidance of the Business Program Manager. The Business Project Manager is the single point of contact for the business user community to coordinate clear articulation of requirements, design of user interfaces and business logic, user acceptance testing, involving the Information System Owner (ISO) for defining cybersecurity requirements, design, and testing. The Business Project Manager is responsible for consistently communicating with the user community, building business consensus, and making decisions throughout the project life cycle.

(7) **Integrated Program Team (IPgT).** IT and Business Program Managers have the delegated authority from the CIO, CXO, and their leadership

(Department Directors) to form, maintain and co-lead the IPgT. IPgTs are collectively accountable for performing activities related to planning, management, implementation and operation of an IT Program in PBGC's IT Portfolio. The IPgT includes the IT Program Manager, Business Program Manager, Chief Enterprise Architect, Contracting Officer, Information System Security Manager (refer to PBGC Directive IM 05-02, PBGC Information Security Policy), and impacted stakeholders as necessary. Individual members of the IPgT are accountable for effectively representing their constituent organizations/functions, assign back-up representatives, actively participate in the IPgT to reach consensus and decisions in the best interest of the Program and PBGC success, coordinate and directly perform activities assigned to them (reach back for additional resources necessary from their constituent organizations), keep their constituent leadership team informed and seek input/concurrence on the IPgT activities/decisions.

(8) **Integrated Project Team (IPT).** Integrated Project Teams (IPTs) are formed at the discretion of the Program Managers, maintained and co-led by the IT and Business Project Managers. IPTs are collectively accountable for performing activities related to planning, management, implementation and operation of an IT Project in an IT Program. The IPT includes the IT Project Manager, Business Project Manager, Enterprise Architect, representatives from Information System Security Manager (refer to PBGC Directive IM 05-02, *PBGC Information Security Policy*) , and others as necessary such as the Records Officer, Departmental Records Coordinator, Privacy Office, and impacted stakeholders (integration partners, SMEs, other business partners, dev teams, infrastructure teams, etc.) as necessary. Individual members of the IPT are accountable for effectively representing their constituent organizations/functions, assign back-up representatives, actively participate in the IPT to reach consensus and decisions in the best interest of the Project, Program and PBGC success, coordinate and directly perform activities assigned to them (reach back for additional resources necessary from their constituent organizations), keep the Program Managers and their constituent leadership team informed and seek input/concurrence on the IPT activities/decisions.

(9) **Contracting Officer (CO).** As the acquisition expert, ensures compliance with Federal Acquisition Regulations and applicable PBGC clauses. Develops and approves the IT Program Acquisition Strategy. Partners with EA to determine product selection strategies. Facilitates the team through the acquisition process and participates on IPgTs.

(10) **Enterprise Architect (EA).** As an active participant, facilitates the development of Business Needs Analyses. Represents an enterprise perspective, provides recommendations for platform/service reuse, technology choices, design reviews, and adherence to IT Standards.

(11) **Release Manager/Analyst (RM/A).** As the single point of contact to the IT Infrastructure, facilitates the implementation of IT Solutions through

development, test, production and COOP environments. Engineers and designs the best IT Infrastructure footprint for the IT solution. The RM/A guides the teams through IT Infrastructure processes, Release and Change Management processes, and coordinates with members of ITIOD.

(12) **Records Officer and PBGC Departmental Records Coordinators.** Review PBGC records, file plans, and other records management artifacts to define records retention and archival requirements in accordance with the Requirements Standard for IT solutions/systems. Ensure the retention and archival requirements are implemented in the IT solutions/systems.

Note: Above are a list of roles and responsibilities that are critical to the success of this Directive. It is permissible (especially in small programs) for a single individual to hold multiple roles at once. Care should be taken to avoid conflicts of interest. The CIO and CXOs are responsible for mitigating conflicts of interest.

10. **PROCEDURES**: Processes, procedures, and supplemental documents are located on the Information Technology Intranet Site or can be provided upon request.

- **Glossary of Terms**
- **IT Portfolio Review Board**
- **IT Solutions Life Cycle Management**
- **Technical Review Board**
- **Technical Reference Model**