Pension Benefit Guaranty Corporation

Office of Inspector General

Audit Report

PBGC Began Developing Methods for Oversight and Administration of Cloud Computing Service Providers – Work is Needed for the Expected Increase in Externally Hosted Systems

August 6, 2015

AUD-2015-11/PA-14-100

Pension Benefit Guaranty Corporation
Office of Inspector General
1200 K Street, N.W., Washington, D.C. 20005-4026

August 6, 2015

To: Alice Maroni
Acting Director

From: Rashmi Bartlett
Assistant Inspector General for Audit

Subject: PBGC Began Developing Methods for Oversight and Administration of Cloud Computing Service Providers – Work is Needed for the Expected Increase in Externally Hosted Systems (AUD-2015-11/PA-14-100)

I am pleased to transmit the final Office of Inspector General (OIG) report on the Pension Benefit Guaranty Corporation's (PBGC) efforts to adopt cloud computing technologies. We recommended that PBGC establish criteria, standards, and definitions to identify cloud service providers and procure vendors with a standard risk-based approach. We also recommended the establishment and implementation of controls along with periodic monitoring of monthly staffing reports to provide reasonable assurance that foreign personnel with access to PBGC data receive the appropriate background checks. Overall, PBGC agreed to take action on all recommendations by March, 2016.

We appreciate the cooperation that OIG received while performing this audit.

cc:
Bob Westbrooks
Bob Scherer
Edgar Bennett
Patricia Kelly
Cathleen Kronopolus
Ann Orr
Michael Rae
Sandy Rich
Judith Starr
Marty Boehm

Executive Summary

The Pension Benefit Guaranty Corporation (PBGC) has not yet established a cloud computing program with adequate controls, assigned duties, and well-planned oversight of cloud service providers. Because PBGC officials rely on the National Institute of Standards and Technology (NIST) definition of cloud computing, they lack their own set of standard criteria to properly identify the cloud service providers who supply independent operations and services external to the PBGC environment. This condition presents risks to PBGC which require an early identification and definition of cloud boundaries to pave the way for well-defined contractual considerations and successful mitigation of risks. Because this process is not yet in place, PBGC officials reported that one of its vendors refused to obtain FedRAMP certification, a key government control, because the vendor did not believe itself to be a cloud service provider. Until PBGC ensures a cloud computing program is firmly in place, contracts and vendors that should be administered as cloud service providers, may not receive the necessary oversight and scrutiny to ensure the security of PBGC data.

Overall we determined:

- The Corporation will need to ensure critical clauses are included and monitored in cloud computing contracts.
- PBGC officials did not consider how they would identify non-U.S. based personnel in cloud service contracts and verify background checks to provide assurance that all contract personnel met federal requirements and PBGC policy.

We recommended that PBGC establish criteria, standards, and definitions to identify cloud service providers and procure vendors with a standard risk-based approach. PBGC should also establish a multi-disciplinary cloud services procurement team to monitor purchases and ensure contracts include clauses needed to protect the Corporation. We also recommend the establishment and implementation of controls along with periodic monitoring of monthly staffing reports; this will provide reasonable assurance that foreign personnel with access to PBGC data receive the appropriate background checks.

Agency Response:

PBGC has agreed to take action on all the recommendations in this report.

OIG Evaluation:

OIG looks forward to reviewing PBGC's corrective actions, according to PBGC all recommendations in this report will be resolved by March 2016.

Table of Contents

ABBREVIATIONS

Acronyms

ATO……..……...Authorization to Operate

CIGIE…….Council of Inspectors General on Integrity and Efficiency

CFR……..…Code of Federal Regulations

COTS……..Commercial Off-The-Shelf

CSP……Cloud Service Provider

DHS……...United States Department of Homeland Security

DOD……United States Department of Defense

EEO……..Office of Equal Employment Opportunity

ERISA…….….Employee Retirement Income Security Act of 1974

FAR……..… Federal Acquisition Regulation

FedRAMP…….The Federal Risk and Authorization Management Program

FOD……..Financial Operations Department

GSA…….United States General Services Administration

HSPD-12…….Homeland Security Presidential Directive 12

IT…….Information Technology

JAB……...Joint Authorization Board

No FEAR Act.....The Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002

OGC……Office of the General Counsel

OIG…….Office of Inspector General

OMB……...Office of Management and Budget

PBGC……Pension Benefit Guaranty Corporation

PII……...Personally Identifiable Information

NIST……National Institute of Standards and Technology

SLA……..Service Level Agreements

BACKGROUND AND OBJECTIVES

Background

The Pension Benefit Guaranty Corporation (PBGC or the Corporation) is a Federal government Corporation established under Title IV of the Employee Retirement Income Security Act (ERISA) of 1974 to protect the retirement income of individuals and their beneficiaries who are covered under certain private sector, defined benefit pension plans. PBGC's strategic goals are to 1) Preserve pension plans and protect pensioners, 2) Pay timely and accurate benefits, and 3) Maintain high standards of stewardship and accountability. PBGC protects basic pension benefits for about 41 million American workers in nearly 24,000 private pension plans. Information Technology is a cornerstone of PBGC's operations.

In support of the Corporation's mission to meet operational standards, one of the goals listed in PBGC's IT Strategic Plan FY 2014-2018 is to modernize and innovate PBGC's IT solutions through the use of cloud computing and shared services to enable a flexible, reliable, secure, and cost effective environment.[1] PBGC believes cloud computing will offer the potential for significant cost savings through faster deployment of computing resources, decreased need to buy hardware or build data centers, and enhanced collaboration capabilities. Moreover, the Office of Management and Budget (OMB) has also required agencies to adopt a 'Cloud First' policy when considering IT purchases and evaluate secure, reliable, and cost-effective cloud-computing alternatives when making new IT investments.

Cloud computing is a term used to define information technology systems, software, and/or infrastructure that are packaged and sold to customers by an external service provider. National Institute of Standards and Technology (NIST) describes cloud systems as having five essential components,[2] which are:

- On-demand self-service: The customer is able to unilaterally provision computing capabilities with the service provider, as needed, without requiring human interaction.
- Broad network access: The capabilities (storage, servers, databases, etc.) of the service provider are accessed by the customer through a network connection.
- Resource pooling: The customer shares vendor services with other customers.
- Rapid elasticity: The service provider's system allows the customer to rapidly expand or contract required computing resources.
- Measured service: The customer's payment for use of the cloud system is determined by a measured capability, appropriate to the type of service (e.g., storage, processing, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

[1] Information Technology Strategic Plan FY 2014-2018 v 1.1, December 31, 2013.

[2] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011.

The recent initiatives to leverage cloud service providers prompted the Council of Inspectors General on Integrity and Efficiency (CIGIE) IT Committee to commence a Government-wide initiative to assess the efforts of selected agencies implementation cloud-computing technologies. Nineteen Offices of Inspectors General (OIG) participated in the consolidated Cloud Computing initiative. CIGIE based its government-wide report on a sample of 77 commercial cloud contracts issued by federal agencies transitioning to a cloud system, with a value of approximately $1.6 billion (from a universe of 348 contracts totaling $12 billion).[3]

PBGC OIG and other participating OIGs completed a common matrix and audit program provided by CIGIE. After responding to specific questions in the matrix, we timely submitted our responses for inclusion in CIGIE's report. At the time of our review, PBGC reported its inventory of IT cloud computing consisted of two providers, valued at nearly $5.7 million, referred to in this report as cloud service provider (CSP) 1 and CSP 2.

Cloud Service Provider 1 (CSP 1)[4]

PBGC's Financial Operations Department (FOD) prepares the agency financial statements and administers the Corporation's financial and accounting programs. FOD uses an application hosted by CSP 1 to record the transfer of plan assets from a plan's interim custodian bank to PBGC's custodian bank until all plan assets have been received and commingled with other PBGC managed assets. In general, CSP 1 supports PBGC with an investment portfolio application and accounting solution designed to support the accounting and financial reporting of investment assets, plan receivables, and liabilities related to terminated pension plans. This is a commercial off-the-shelf (COTS) product which has been modified to meet PBGC's needs.

Cloud Service Provider 2 (CSP 2)

The Office of Equal Employment Opportunity (EEO) supports PBGC by providing the integration of Federal sector EEO requirements[5] (Title 29 Code of Federal Regulations (CFR) Part 1614[6]) throughout the agency work environment. CSP 2 provides a fully-managed support infrastructure service to PBGC-EEO as well as providing EEO Program Management services to 40 other federal agencies. CSP 2 supports an application that assists EEO personnel in managing and reporting on the overall EEO program. The system provides the capability to monitor the EEO complaints process and assures that PBGC meets established regulatory requirements by

---

[3] The total sample of commercial cloud contracts reviewed by the 19 OIGs was 77. However, the applicability of each question varied by contract. This resulted in a total response of less than 77 for some questions.

[4] During our audit field work, PBGC, through the former Chief Information Officer (CIO), identified CSP 1 as a cloud system. The current CIO informed the OIG that CSP 1 will be reclassified as a managed service.

[5] It is the policy of the Government of the United States to provide equal opportunity in employment for all persons, to prohibit discrimination in employment because of race, color, religion, sex, national origin, age, disability, or genetic information and to promote the full realization of equal opportunity through a continuing affirmative program in each agency. Title 29 Code of Federal Regulations (CFR) Part 1614 Subpart A—Agency Program To Promote Equal Employment Opportunity

[7] EEOC's Office of Federal Operations (OFO) produces an Annual Report on the Federal Workforce that includes, among other data, information on federal equal employment opportunity complaints and Alternative Dispute Resolution activities. This data is collected from each agency in the Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEOC Form 462).

generating an electronic Form 462[7] and No FEAR[8] reports. The application includes a web-based component.

Objectives

We evaluated PBGC's efforts to adopt cloud-computing technologies and reviewed two of the Corporation's cloud service contracts for compliance with applicable standards. We conducted this audit in conjunction with a Government-wide initiative by the Council of the Inspectors General on Integrity and Efficiency. We elected to prepare this separate report and further elaborate on PBGC-specific findings and recommendations.

[7] EEOC's Office of Federal Operations (OFO) produces an Annual Report on the Federal Workforce that includes, among other data, information on federal equal employment opportunity complaints and Alternative Dispute Resolution activities. This data is collected from each agency in the Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEOC Form 462).

[8] The Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 became effective on October 1, 2003. The Act requires Federal agencies to be accountable for violations of antidiscrimination and whistleblower protection laws, in part by requiring that each Federal agency post quarterly on its public Web site, certain statistical data relating to Federal sector equal employment opportunity complaints filed with each agency. An agency must submit to Congress, EEOC, the Department of Justice, and OPM, an annual report setting forth information about the agency's efforts to improve compliance with the employment discrimination and whistleblower protection laws and detailing the status of complaints brought against the agency under these laws.

AUDIT RESULTS

Finding 1: PBGC Has Not Developed Standards and Criteria to Identify Cloud Service Providers and Lacks a Framework to Ensure Critical Clauses are Included and Monitored in its Cloud Contracts.

PBGC did not have established standards and criteria for identification of cloud service providers. Further, PBGC has not fully defined roles and responsibilities for ensuring critical clauses are included and monitored in cloud computing contracts. This occurred because PBGC's process for managing cloud service providers has not matured. PBGC has not established policies and procedures for the oversight and maintenance of cloud computing contractors, including identifying boundaries and parameters that define cloud service providers. As a result, contracts and vendors that should be administered as cloud service providers may not receive the appropriate oversight and scrutiny to ensure the security of PBGC data. For example, PBGC classified CSP 1 as a cloud service provider; however, the vendor representatives adamantly asserted they were not a cloud service provider and therefore would not be seeking FedRamp compliance, a key control for federal government cloud services.

We initiated the audit through an inventory request of cloud systems within the PBGC environment. PBGC sought clarification regarding our definition of a cloud system. We referred to the NIST definition[9] used by CIGIE, and the Corporation informed us that they adopted the same definition. PBGC officials stated that although the two systems met elements of the NIST characteristics of cloud systems, they did not meet all of them as a "true cloud" system. Nonetheless PBGC considered them to be cloud service providers. We observed that other government agencies had similar difficulties identifying and classifying cloud systems, as noted in CIGIE's Government-wide audit report on cloud computing:

> … Many of the agencies that participated in the initiative had difficulty obtaining an accurate cloud system inventory due to a failure by agencies to report all cloud systems and a lack of consistency in applying cloud definitions.

[9] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011.

"Cloud computing is 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, three service models, and four deployment models."

The NIST definition provides a helpful roadmap for agencies; however, a more distinct and perhaps agency-specific definition for a cloud computing vendor would be beneficial as PBGC considers moving additional services to the cloud. A unified definition would help PBGC identify and address future situations early in the process where the government and vendor designation of a CSP differ. CSP 1 did not consider itself to be a cloud service provider because PBGC is their only government client. PBGC, on the other-hand, considered the vendor to be a cloud service provider given that the data was external and not housed in the PBGC environment; the provider built the application and maintains all hardware and software at off-site locations. A company that does not operate as a CSP can present challenges for PBGC; most significantly, CSP 1 informed OIG that they would not seek FedRamp compliance.[10]

FedRAMP was introduced on December 8, 2011, via an OMB policy memo, which addressed the security authorization process for cloud computing services. It provides an important baseline for security requirements; OMB requires each executive department or agency to use FedRAMP when conducting risk assessments, security authorizations, and granting an Authorization to Operate (ATO) for use of cloud services. FedRAMP provides a cost-effective, risk-based approach for the adoption and use of cloud services. It includes:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;[11]
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs;
- Authorization packages of cloud services reviewed by the Joint Authorization Board (JAB) consisting of security experts from Department of Homeland Security (DHS), Department of Defense (DOD), and General Services Administration (GSA);[12]
- Standardized contract language to help executive departments and agencies integrate FedRAMP requirements and best practices into the acquisition of cloud systems; and
- A repository of authorization packages for cloud services that can be leveraged government-wide.

A lack of conformity and consistency in deploying and assessing cloud service providers presents risk to PBGC. Although CSP 1 completed a NIST 800-53 controls assessment – which

[10] In its government-wide report, CIGIE reported that 60 agency systems they reviewed failed to achieve FedRAMP compliance.

[11] The system's security category is determined in accordance with Federal Information Processing Standard 199 impact level categories of low or moderate. After the category is determined, the contractor shall apply the appropriate set of baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance with security standards. The FedRAMP baseline controls were based on NIST SP 800-53, Revision 3.

[12] Authorization packages contain evidence needed by authorizing officials to make risk-based decisions regarding the information systems that are providing cloud services. This includes, as a minimum, the security plan, security assessment report, plan of action and milestones, and a continuous monitoring plan.

includes an evaluation of many important controls – and PBGC granted this provider an ATO.[13] FedRAMP addresses the unique control challenges that cloud services present; contracts must be negotiated carefully for critical elements such as service levels and compliance with federal laws. FedRAMP compliance ensures that cloud-based services have an adequate information security program that addresses the specific characteristics of cloud computing and provides the level of security necessary to protect government information.

OIG and agency access to cloud data is an emerging issue within the federal sector. CIGE found in its government-wide consolidated final report:

- 61 contracts reviewed did not include language to allow agencies to conduct forensic investigations for both criminal and non-criminal purposes without interference from the CSP.
- 65 contracts did not detail procedures for electronic discovery when conducting a criminal investigation.
- 54 contracts did not include language to allow the OIG full and unrestricted access to the contractor's (and subcontractor's) facilities, installations, operations, documentation, databases, and personnel used in performance of the contract in order to conduct audits, inspections, investigations, or other reviews.

Although contracts (within our sample) had the appropriate FAR clause provisions regarding access, we determined that PBGC has not established adequate Corporate-wide controls to ensure OIG and agency access to cloud data. For example the contract for CSP 1 expressly stated and included clauses to ensure access. However for CSP 2, the language ensuring access was included in another overarching contract vehicle referred to as STARS I, which incorporated more than 80 FAR clauses by reference. PBGC must ensure controls and procedures are consistently applied and maintained, which clearly allow for OIG and agency access to government data in the cloud. Without adequate contracting provisions, PBGC risks escalating cost for e-discovery, audit and investigative services.

PBGC should develop a team of technically proficient personnel to develop a cloud definition for the Corporation, which includes definitive criteria from which the agency will make such determinations prospectively. The agency should also develop a cloud working group to assess potential cloud computing vendors, and those discussions should include a determination of whether the vendor considers itself a CSP. Upon making these determinations, PBGC should have an established course of action from which to make their procurement decisions. PBGC should also consider developing a checklist or other formally documented control that matures over time to appropriately query vendors and capture adequate contractual provisions that will ensure agency and OIG access. This should also include controls for consistent contract language that will protect PBGC from inflated or ballooning costs which can rapidly occur under poorly or hastily-developed cloud contracts. PBGC's cloud working group should be comprised of

[13] Not all externally hosted services are cloud based, nor fall under the purview of FedRAMP. FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

personnel from IT, procurement and OGC – three critical entities whose coordination is essential to ensure cloud contracts deliver cost-effective services that protect the interests of the Corporation.

Recommendation 1 (OIT-147): Establish criteria, standards, and definitions to identify cloud service providers and procure vendors with a standard risk-based approach so that cloud contracts are consistently identified and administered in a manner that protects PBGC data.

Recommendation 2 (OIT-148): Establish a multi-disciplinary cloud services procurement team that includes assigning roles and responsibilities to PBGC personnel in IT, procurement, and OGC to monitor purchases so that contracts include clauses needed to protect PBGC information and systems.

Agency Response:
PBGC does not agree with language in this finding; however, the Corporation agrees in principle with both recommendations regarding additional work needed to implement a more robust cloud computing framework.

OIG Evaluation:
OIG looks forward to reviewing PBGC's corrective actions by March 2016.

Finding 2: PBGC Did Not Obtain Documented Assurance that a Cloud Provider Performed Background Checks on Non-U.S. Based Personnel with Access to PBGC Information and Systems.

PBGC did not obtain documented assurance that CSP 1 conducted background checks on non-U.S. based personnel with elevated privileges and super user access to PBGC data and information. This occurred because PBGC did not ensure that the contract contained language allowing PBGC to obtain the necessary documentation supporting the CSP's performance of adequate background checks. Additionally, PBGC's background investigation requirements did not address non-U.S. based personnel working under cloud computing contracts. As a result, PBGC could not provide assurance that its data and networks are protected against potential threats and vulnerabilities associated with CSP 1's reliance on non-U.S. based personnel.

Homeland Security Presidential Directive 12 (HSPD-12) directs U.S. government agencies to establish minimum background screening requirements in order to issue access credentials. HSPD-12 primarily deals with physical access to government facilities, with the underlying premise to protect Federal government resources – people and data. PBGC Directive PM 05-6, *Personnel Security and Suitability Program*, requires that all PBGC Federal employees or appointees and Contractors have a background investigation. Computer/IT positions are to receive an additional level of review to assess the risks associated with access to the Corporations computer systems. As the government moves to a cloud environment where physical IT equipment and data will be stored off-site and accessed by foreign nationals, government agencies must also take the same precautions and should strive to meet the intent of HSPD-12.

Background checks on individuals living within the United States who have physical and logical access to government systems and data present challenges. These same challenges are magnified when attempting to perform background checks on foreign nationals. Government contracts typically do not provide guidance regarding the processes to be used or the depth of the investigations to be conducted, leaving the contractor to determine how to conduct the background screening. For example, a contractor may engage a screening company to conduct the foreign national background check; the screening may not include a court records review for criminal or negative financial information if not directed to do so.[14] Moreover, privacy laws in foreign countries can restrict access to criminal records. Other barriers to conducting foreign background checks include:

[14] Screening companies may not review Federal/state court records if not directed to do so and background screening firms generally only check the records of the court that maintains the preponderance of criminal data - - this could lead to missing records maintained by specialized courts, such as domestic or family law courts. According to GAO, one official from a background screening firm explained that only some of the 88 counties in Ohio report crimes to the state repository, per GAO-0699R. Similarly, the state of Illinois reported that in 2003, only 59 percent of the computerized criminal history records they audited had complete information, per GAO-0699R.

- Applicant- provided information may be unreliable and inaccurate information. Since some countries, such as India, have no national criminal database and maintain criminal data at the local level, background screenings may miss crimes committed in other locations within the country if the applicant did not reveal all previous addresses.
- Some countries lack national identification numbers. Without a unique identification number, a screener may not be able to determine just by name if a person committed the crimes cited in the court or police records.
- Criminal records may be unreliable. Because some countries experience high levels of corruption, records might not be created or may be modified due to monetary incentives or inappropriate political influence.

OIG met with PBGC and CSP 1 on numerous occasions to obtain documentation supporting completed background checks performed on more than 80 foreign national personnel who have help desk, system administrator and key security roles (note: CSP 1 and PBGC reported that the CSP, not PBGC, completed the background checks). In response to OIG's first request, PBGC provided the contractor's vetting process for non-U.S. based personnel. PBGC then provided documentation of the background process along with a sample background check. After more persistent requests, PBGC informed us that since background checks of foreign personnel were highly confidential, no further details would be provided.

We then asked if hard copy documents (for viewing purposes only) could be provided during our site visit to CSP 1. We explained to CSP 1 that we only wanted to view the documents and they would not be retained or copied; CSP 1 denied our request. We requested redacted documents which could be provided or simply displayed on screen; the CSP also denied this request. Despite these setbacks, we continued efforts to work with CSP 1 on a method to demonstrate that the background checks for more than 80 non-U.S. based personnel with key roles had been completed and reviewed for suitability for employment. Consistent denials at every request raised concerns.

More than two months after our initial request, PBGC then stated that they were pleased to provide background screening documentation. They reported CSP 1 provided them with what they termed as a "scrubbed background screening document" of one CSP employee. However, upon our review of this single report, we found it did not contain any pertinent information that PBGC could use to reasonably determine that background checks were performed on the more than 80 non-U.S. based personnel. This issue is particularly concerning considering PBGC's lack of monitoring of CSP 1's non-U.S. based personnel:

- From November to December 2013, CSP 1 doubled its non-U.S. based personnel without documented notification to PBGC through required monthly reports.
- Seven monthly contractor staff reports for CSP 1 did not consistently report staff locations and risk levels were inappropriately assigned to some contractors. Though CSP 1 listed one employee in all 7 reports, PBGC later determined the employee did not even work on the PBGC project. As a result of our inquiries, the employee was removed from the listing in May 2014.

Alluding to the challenges that arise when performing background checks, the scrubbed document contained the following disclaimer:

> …the information made available to us by such authorities is produced "as is"; therefore, we cannot guarantee the accuracy of information collected. …Also, due to factors beyond our control it may not be possible for us to procure all the necessary information.

Another clause in the scrubbed document barred distribution of the background check and presented an additional roadblock for PBGC's access to the information needed to determine if CSP 1's foreign based staff are suitable for employment and access to PBGC systems and information:

> …these reports are not intended for publication or circulation to any third party including the applicant nor can they be used or reproduced for any other purpose, in whole or in part, without our prior written consent in each specific instance.

Recent fraudulent practices of other background screening companies have come to light which stress the importance of verifying background screening information. The contractor that performed background investigations on Eric Snowden and Aaron Alexis[15] conducted a practice of "dumping," whereby background investigations were not reviewed or not performed in order to maximize profits and "hit revenue."[16] The failure of appropriately rigorous background investigations resulted in these individuals having access to facilities and data which led to the horrific loss of life and unsanctioned release of highly-sensitive information.

PBGC must explore the risks and implement controls to mitigate those risks. Per OMB Circular A-123, *Management's Responsibility for Internal Control*, organization, policies, and procedures serve as internal controls that provide program and financial managers with tools to help achieve results and safeguard the integrity of their programs. Ensuring cloud providers' FedRAMP compliance provides one of those tools for PBGC management. This is critical as the agency considers moving more resources to the cloud, some of which will contain sensitive information, including participant Personally Identifiable Information (PII). The inherent risks and challenges of background checks for foreign employees are exacerbated when a contractor is unwilling to share documentation of the due diligence. PBGC must ensure future contracts include strong language that allows corroboration of background check information on all personnel with access to PBGC data or systems, including third party-managed environments and support functions. PBGC and the OIG must have full unencumbered access to the documentation that supports completion of the background checks, including access to source documents.

Recommendation 3 (OIT-149): Establish, implement and monitor controls which provide reasonable assurance that foreign personnel with access to PBGC data and information systems receive background checks in accordance with PBGC policy and procedures.

---

[15] Eric Snowden released classified information regarding the National Security Agency program. Aaron Alexis perpetrated the Washington Navy Yard shooting.

[16] According to a Staff Report from the Committee on Oversight and Government Reform, February 11, 2014, the contractor "dumped" approximately 665,000 background investigations or 40% of its total investigations conducted over a four year period.

Recommendation 4 (OIT-150): Improve controls over monitoring by enforcing review of monthly staffing reports for accuracy and periodic security categorization.

Agency Response:
PBGC does not agree with this finding, the agency believes the provider (CSP 1) is a non-cloud based managed service provider, not a cloud provider. PBGC does agree with the need to ensure foreign personnel with access to PBGC data and information systems receive background investigations in accordance with PBGC policy and procedures.

OIG Evaluation:
At the initiation of our audit we requested an inventory of cloud service providers; PBGC listed CSP 1 as a cloud service provider. In September, 2015 PBGC expects to submit evidence to support the closure of recommendations 3 and 4, OIG looks forward to reviewing PBGC's corrective actions.

APPENDIX A: SCOPE AND METHEDOLOGY

Scope

We performed fieldwork between January and June 2014, at PBGC headquarters in Washington, D.C., and conducted site visits to two cloud service providers (located in Pennsylvania and Virginia). We began with a generic audit template provided by CIGIE and tailored it to PBGC. This scope addresses work conducted for both the CIGIE report and this PBGC OIG specific report. We reviewed two CSPs, which encompassed PBGC's entire inventory of CSPs. Though PBGC fully expected to move additional services such as email to the cloud, agency officials reported that the two systems submitted in the survey represented PBGC's entire cloud environment at the time of survey in FY 2014.

We evaluated PBGC's efforts to adopt cloud-computing technologies in a manner that complies with current guidance, including a joint publication from the Chief Information Officers Council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*, Federal Risk and Authorization Management Program (FedRAMP), Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors*, NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, OMB Federal Cloud Computing Strategy, Federal Acquisition Regulation, Inspector General Act, and OMB Circular A-123, *Management's Responsibility for Internal Control*. We reviewed applicable PBGC policies and procedures, as well as both CSP contracts and other relevant documentation.

Methodology

We conducted this review as part of a CIGIE initiative to review cloud computing, and timely provided our results via a matrix to USDA OIG, CIGIE's audit control point. CIGIE consolidated the results into a report that assessed cloud computing government-wide, and we elected to prepare this report specific to PBGC – this methodology addresses work conducted for both reports. We conducted a survey of PBGC's enterprise-wide inventory of Cloud IT services and service providers in FY 2014 and judgmentally selected the only two CSPs submitted in the agency's response to the survey. We reviewed the contracts executed between PBGC and the two CSPs to determine whether they contained key content such as:

- clearly defined roles for PBGC, and the CSP;
- Federal Acquisition Regulation clauses for access to CSP facilities and specific details addressing investigative, forensic, and audit access; and
- terms to obtain sufficient documented assurance that background checks for Non-U.S. based personnel were conducted.
- We reviewed service level agreements (SLA) with the CSPs to determine whether the SLA defined performance with clear terms and definitions (uptimes, etc.), demonstrated

how performance was measured, and defined enforcement mechanisms when performance standards were not met. In order to determine if PBGC centrally manages contracts, we reviewed cloud service providers and related documentation for the CSP contracts and interviewed personnel within the Office of Information Technology and Procurement Department, as well CSP representatives and users that interact with the cloud applications on a day-to-day basis. We compared the cloud service documentation to recommended best practices for contracts and SLA monitoring to determine whether PBGC had a process in place to effectively manage its cloud computing providers to ensure contractual obligations were met.

For the CSPs selected, we reviewed evidence of compliance with applicable criteria such as the Federal Risk Authorization and Management Program (FedRAMP), National Institute of Standards and Technology (NIST) guidance, and OMB Circular A-123, *Management's Responsibility for Internal Control*.

This audit was conducted in accordance with generally accepted government auditing standards. The standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. The evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: AGENCY RESPONSE

PBGC
Protecting America's Pensions

Pension Benefit Guaranty Corporation
1200 K Street, N.W., Washington, D.C. 20005-4026

To: Robert A. Westbrooks, Inspector General

From: Alice C. Maroni, Acting Director

Subject: Response to Draft OIG Report Regarding Cloud Computing

Date: July 24, 2015

We appreciate the opportunity to comment on OIG's draft Cloud Computing Report. PBGC's cloud computing efforts are still nascent – the Corporation has only one cloud-based service that is relatively minor (an EEO complaints system that is in use throughout the Federal Government); a second is in development. PBGC's Office of Information Technology has been working to put a framework in place, including learning the NIST definitions and standards applicable to cloud computing, as well as analyzing risks and potential risk mitigation strategy. We intend to take a slow and careful approach to the cloud and look forward to consulting with OIG as we move forward to ensure that PBGC data are properly protected.

PBGC's Office of Information Technology is comfortable with the National Institute of Standards and Technology's (NIST) definition of cloud computing and intends to follow it rather than create an agency-specific definition. We believe that a proliferation of definitions would cause confusion and undermine NIST standard-setting. Indeed, given the fact that some agencies are offering multi-agency vehicles for cloud computing, we are concerned that a lack of uniformity could cause agencies to categorize differently the identical service.

As the Report notes (footnote 13), not all externally hosted services are cloud-based. According to NIST, the cloud model is composed of five essential characteristics: on-demand self-service, resource pooling, broad network access, rapid elasticity, and measured service.[1] Cloud based services can be delivered through shared service agreements with other agencies, or managed service agreements with commercial providers, but these arrangements are not cloud-based unless they meet the NIST definition.[2] At the outset of this audit engagement, there was some confusion about one of PBGC's managed services (referred to as CSP 1 in the report); after a thoughtful analysis of the NIST standard, we are comfortable it is a non-cloud based managed service.

---

[1] Excerpted from: *The NIST Definition of Cloud Computing*, NIST SP 800-145; September 2011.

[2] Derived from: OMB's *Federal Information Technology Shared Services Strategy; May 2012.*

For its one cloud service, PBGC is using, and intends to use for all future efforts, cloud services providers that are Federal Risk and Authorization Management Program (FedRAMP) compliant. That is the case for the EEO service and for the PBGC Connect effort that will support email, file sharing, and other commodity-type services in the cloud.

PBGC employs the appropriate FAR clauses in its individual contracts. It is important to understand that PBGC may use existing Government Wide Acquisition Contracts (STARS II small business set-aside) to procure cloud-based services. Part of the value of such contracts is that they already have the appropriate FAR clauses embedded in them. For PBGC to build the same clauses into an agency-specific contract would be duplicative and eliminate some of the value of using a GSA vehicle. PBGC may also use shared services agreements implemented through inter-agency agreements, which are not subject to the FAR. Instead, PBGC will ensure that the counterpart agency has included the appropriate clauses in its contracts.

We agree that the use of foreign personnel creates a unique set of challenges and in response the PBGC issued Directive Number GA-10-12 – *Guidelines for the Use of Foreign Nationals in PBGC Contracts* on June 15, 2015 to address the use of foreign personnel in support of PBGC contract activities. In addition to providing overall guidance for all procurement actions which involve contracting with companies who may employ foreign nationals residing and performing PBGC services outside the U.S. and its territories, it specifically provides policy and procedural guidance on conducting and adjudicating background investigations on foreign personnel, as well as continued management of risk throughout the life of the contract.

Please find our responses to individual findings and recommendations included in the draft report below:

Finding 1: PBGC Has Not Developed Standards and Criteria to Identify Cloud Service Providers and Lacks A Framework to Ensure Critical Clauses are Included and Monitored in its Cloud Contracts.

Recommendation 1 (OIG Control Number): Establish criteria, standards, and definitions to identify cloud service providers and procure vendors with a standard risk-based approach so that cloud contracts are consistently identified and administered in a manner that protects PBGC data.

Recommendation 2 (OIG Control Number): Establish a multi-disciplinary cloud services procurement team that includes assigning roles and responsibilities to PBGC personnel in IT, procurement, and OGC to monitor purchases so that contracts include clauses needed to protect PBGC information and systems.

Agency Response:

While we do not agree with the language of the finding (see the discussion in the previous section explaining the definitional and contracting issues), we agree in principle with both recommendations regarding additional work we need to do in implementing our framework. With respect to Recommendation 1, OIT is in the process of updating a number of internal documents to codify the definition of cloud computing (NIST definition) and the three basic methodologies to provide IT based systems and services; 1) shared services, 2) managed services, and 3) in-house PBGC provided. As

noted earlier, OIT follows a risk based approach to providing IT services and support and will continue to do so in the future. One aspect of that risk based approach will be to utilize only FedRAMP compliant cloud service providers (CSPs) for shared or managed service based cloud solutions. The expected timeline for implementation of Recommendation 1 is March 31, 2016. With respect to Recommendation 2, OIT will lead the establishment of a multidisciplinary team that will include members from OIT, the Procurement Department (PD), and the Office of the General Counsel (OGC). This team will review existing acquisition policies, procedures, and processes for cloud-based solutions and make any necessary changes. The team will also develop checklists for each type of procurement activity and/or update existing checklists as needed, understanding, as explained above, that different contracting vehicles require different approaches.

The expected timeline for submitting evidence of work completed on Recommendations 1 & 2 is March 31, 2016.

Finding 2: PBGC Did Not Obtain Documented Assurance that a Cloud Provider Performed Background Checks on Non-U.S. Based Personnel with Access to PBGC Information and Systems.

Recommendation 3 (OIG Control Number): Establish, implement and monitor controls which provide reasonable assurance that foreign personnel with access to PBGC data and information systems receive background checks in accordance with PBGC policy and procedures.

Recommendation 4 (OIG Control Number): Improve controls over monitoring by enforcing review of monthly staffing reports for accuracy and periodic security categorization.

Agency Response:

We do not agree with this finding, as the provider under discussion is a non-cloud based managed services provider, not a cloud provider. We do agree with the need to ensure that foreign personnel with access to PBGC data and information system receive background investigations in accordance with PBGC policy and procedures as noted in Recommendation 3. We believe that PBGC now has in place processes to deal with this issue. On June 15, 2015, PBGC issued Directive Number GA-10-12 – *Guidelines for the Use of Foreign Nationals in PBGC Contracts* to address the use of foreign personnel in support of PBGC contract activities. In addition to providing overall guidance for all procurement actions which involve contracting with companies who may employ foreign nationals residing and performing PBGC services outside the U.S. and its territories, it specifically provides policy and procedural guidance on conducting and adjudicating background investigations on foreign personnel, as well as continued management of risk throughout the life of the contract.

It should be noted, that where PBGC did enter into a cloud based contract for email and other commodity services (the upcoming PBGC connect effort), it deliberately and specifically took steps to ensure that only U.S. based resources and facilities would be used to support the effort and that personnel used to support the system(s) would be U.S. citizens. Therefore, we believe that issues regarding personnel do not exist in our current and forthcoming cloud computing contracts, and that we are well placed to address them in any future contracts.

If the OIG experiences difficulty in obtaining documentation and/or information, we encourage the OIG to reach out to the appropriate C-level staff, so that the issue can be resolved in a timely manner.

With respect to Recommendation 4, Directive Number GA-10-12 – *Guidelines for the Use of Foreign Nationals in PBGC Contracts* would serve as the basis for actions to ensure the continued management of risk throughout the life of any cloud based contract where foreign nationals are present.

In summary, a number of changes have occurred since the cloud audit was undertaken. These changes include: a new Chief Information Officer, adoption of clear definitions for cloud, shared, and managed services; a revised and reduced focus on the use of cloud based solutions; and the development of policies and procedures in the form of Directive Number GA-10-12 – *Guidelines for the Use of Foreign Nationals in PBGC Contracts.* Collectively these changes and the proposed agency responses to Recommendations 1 and 2 address the salient risk management issues raised with respect to the acquisition and use of cloud services, as well as, use of foreign nationals in a support role on any PBGC contract.

The expected timeline for submitting evidence of work completed on Recommendations 3 & 4 is September 30, 2015.

Again, thank you for the opportunity to comment on the draft report, and we will keep the OIG updated regarding the planned corrective actions.

If you want to report or discuss confidentially any instance of misconduct, fraud, waste, abuse, or mismanagement, please contact the Office of Inspector General.

Telephone:
The Inspector General's HOTLINE
1-800-303-9737

The deaf or hard of hearing, dial FRS (800) 877-8339
and give the Hotline number to the relay operator.

Web:
http://oig.pbgc.gov/investigation/details.html

Or Write:
Pension Benefit Guaranty Corporation
Office of Inspector General
PO Box 34177
Washington, DC 20043-4177