PBGC Pension Benefit Guaranty Corporation

Security & Privacy Authorization

One Agency's Tool Based Approach

Shawn A. Hartley, Chief Privacy Officer & Sue Schultz-Searcy, Assessment and Authorization Division Manager
May 26, 2021

The views of Mr. Hartley and Ms. Schultz-Searcy are theirs alone and do not necessarily reflect the views of PBGC.

All remarks are off-the-record and not for attribution.

Introduction to PBGC

- What is PBGC?
  - Pension Benefit Guaranty Corporation (PBGC) established as part of the Employee Retirement Income Security Act of 1974 (ERISA)
  - PBGC protects the pensions of over 34 million Americans
- How does PBGC do Privacy & Security?
  - PBGC has located its Privacy Office within the General Law & Operations Department of the Office of the General Counsel
  - PBGC has located its Security function within the Enterprise Cybersecurity Department (ECD) in the Office of Information Technology
  - Privacy & ECD work closely together (as you'll see)

Introduction to Your Speakers

- Mr. Hartley
  - Joined PBGC as a federal employee in 2002. Has served in various roles within the Office of Information Technology as a Quality Assurance Specialist and performing Audit Coordination.
  - Transitioned to the realm of Privacy and FOIA in 2014.
  - Married the two disciplines of Security Controls assessment with operation of the agency's Privacy Program.
- Ms. Schultz-Searcy
  - After serving in the private sector in IT Security Compliance & Oversight supporting federal clients, joined US Department of Commerce in February 2011.
  - Joined PBGC in November 2016 to serve as the IT Security Compliance & Oversight Program Lead in Enterprise Cybersecurity Division. This included performance of annual Security A&A reviews of all FISMA Reportable Information Systems.
  - Partnered with Privacy Office to rebrand the program Security & Privacy A&A to ensure PBGC is capturing and managing both security and privacy risks.
  - Became Division Manager of Assessment & Authorization Division (AAD) within the Enterprise Cybersecurity Department. Compliance & Oversight work includes input from CSAM, Tenable, Splunk, and other related tools. AAD uses tools including automated dashboard to report and manage IT security and privacy risks and communicate to management.

Risk Management Framework

- Goals of the RMF
  - To improve information security and privacy
  - To strengthen risk management processes
  - To encourage reciprocity among federal agencies

- Implementation of an RMF helps achieve goals, such as:
  - Compliance with federal requirement and guidelines including Federal Information Security Modernization Act (FISMA); OMB A-130.
  - Near real-time analysis of IT security and privacy risks in a state of continuous monitoring.
  - Monitoring and tracking of trends and areas the agency needs to focus additional resources on to achieve best practices.

NIST Risk Management (NIST 800-37 Rev2)

Pension Benefit Guaranty Corporation

PBGC's Risk Management Framework

- The RMF is reviewed and updated annually by the Enterprise Cybersecurity Department and approved by the Cybersecurity & Privacy Council
  - RMF establishes CSAM as the enterprise tool for managing security & privacy for PBGC information systems and instructs use of the tool for system inventory, documentation, POA&M management and management of contractor or cloud systems.
  - RMF establishes that the System Security Plan generated by CSAM is also the System Privacy Plan and the Information System Continuous Monitoring Plan is also the Privacy Continuous Monitoring Plan.
  - RMF establishes that the ISSO role has been renamed to Information System Security & Privacy Officer (ISSPO).

Enterprise Common Controls

- The Enterprise Common Control programs go through their own cycles of RMF, and Continuous Monitoring including assessment of security and privacy controls.
- Enterprise Common Control Program also developed and implemented a Change Management Process through an automated tool that receives and adjudicates requests for changes in common control offerings from systems and Common Control Providers.
- CSAM automatically notifies system owners:
  - A common control is no longer offered
  - A change in the implementation status of common controls
  - POA&M status for Common Controls

Using CSAM for Common Controls

- PBGC also stores its Common Controls Programs in CSAM
  - Allows Common Control Providers to offer controls for inheritance
  - Can put constraints and conditions on inheritance
  - Allows inheriting systems to evaluate the implementation statements and assess the risk of inheritance

Using CSAM as the Agency Repository

- The RMF requires that CSAM be used as the repository for agency information systems. Many documents can be stored on either the Status & Archive pages or the Privacy pages.

- Clear showing of inheritance for controls (and ability to rely upon results for the common controls they are inheriting).

- Prior to using CSAM for system repository A&A packages were generated on paper and stored in binders. System Owners submitted these binders of static documentation for review and recommendations. This led to lengthy review of SSPs associated with the Common Controls, to determine which controls could be inherited.

Core Controls

- Each year, ECD and Privacy Office review Core Controls and determine any changes to those controls based on risk-based analysis. Each core control must be assessed at least annually.

- Selecting core controls each year allows PBGC to put the proper emphasis on the controls that are important to the agency.

- PBGC uses a combination of criteria to determine the controls, such as:
  - Controls related to audit findings so we can understand the weaknesses.
  - Review of overlays and mappings such as the Cyber Security Framework or HVA overlay.
  - Controls that have annual output.
  - Controls that have changed inheritance from common controls to system specific or system specific to common controls.

Ongoing Authorization & Core Controls

- ECD uses CSAM to monitor assessment of core controls and management of risks related to core controls:
  - Monthly reporting on system specific core controls to ensure POA&Ms and risk acceptances are associated with weaknesses.

- To maintain Ongoing Authorization, systems must complete these assessments annually. ECD and Privacy could remove a system from continuous monitoring if Core Controls are not assessed annually.

Post-Assessment Review

- The Security and Privacy A&A team conducts reviews of IT security and privacy risks following the independent assessment of controls but prior to authorization or a decision by an Authorizing Official to continue in ongoing authorization. The team relies on CSAM and other related tools to conduct these reviews.
- The review includes:
  - an overall review of the A&A package including system documentation, assessment of security and privacy controls, and a review of the ISCM plan and process;
  - IV&V of all system specific core controls;
  - a scan of internal information systems and report of any outstanding vulnerabilities not being managed or remediated.
- IT security and privacy risks are identified in the SPA&A report. These risks are outlined in a memorandum from the SAOP & CISO to the Authorizing Official. The SAOP and CISO make a recommendation to the AO on authorization or continuance in ongoing authorization.
- Working with ECD and Privacy, system owners also work on timeframes for implementation of the report recommendations.

Information System Continuous Monitoring

- PBGC's Enterprise Continuous Monitoring Strategy and RMF Process define what a system needs to migrate into and maintain continuous monitoring.
  - Robust ISCM plan aligned to the ECM strategy
  - Annual assessment of Core Controls
  - Assessment of controls at appropriate NIST SP 800-53 revision

- PBGC uses CSAM to monitor compliance with continuous monitoring.
  - Assessment motives used for annual assessment of Core Controls and security and privacy controls outlined within the ISCM plan cycles
  - Updates and annual review of ISCM plans
  - Notification of POA&Ms opened or closed for weaknesses and risks; overdue notifications and reminders

Agency Defined Data Items

- PBGC has written agency defined questions that automatically get attached to information systems.
  - For instance:
    - Is this information a Cloud System?
    - Is the system FedRAMP certified?
    - Does this information store and process SSNs?

- PBGC uses CSAM to track and report these items within FISMA quarterly and annual reporting through System Reports.

Plans of Action & Milestones

- Both systems and Common Control Providers use CSAM to open POA&Ms for remediation of weaknesses.

- Using CSAM, ECD and Privacy can:
  - Track and report monthly trends in open, and delayed POA&Ms and Milestones for Common Control Providers and Information Systems
  - Analyze trends in specific control weaknesses in controls across the agency
  - Track and manage remediation of IT security weaknesses and risks identified in audit recommendations
  - Be responsive to business areas POA&M management issues and concerns

- CSAM automatically notifies system owners of:
  - POA&Ms and Milestones coming due
  - POA&Ms and Milestones overdue

Reporting

- CSAM has a robust set of reports built into the system that can be exported to a variety of formats
- CSAM API works with various reporting tools (i.e. Power BI). Agencies are also able to connect data from CSAM and Archer.
- ECD uses this automation of tools to feed an Enterprise Risk Intelligence Quotient (ERIQ) dashboard to report and monitor different types of risk – System Inventory, POA&M Management; Vulnerability Management; SIM management; Common Controls management; Core Controls management; Agency Risk Management for all domains not just IT Security; and Phishing data.
- Segments of the ERIQ dashboard are shared with CIO/CXO monthly meetings and the dashboard is available for program managers and other businesses for real time views and updates.

Questions?

For official PBGC statements, please contact PBGC Public Affairs at 202-229-4343 or PBGCExternalAffairs@PBGC.gov.