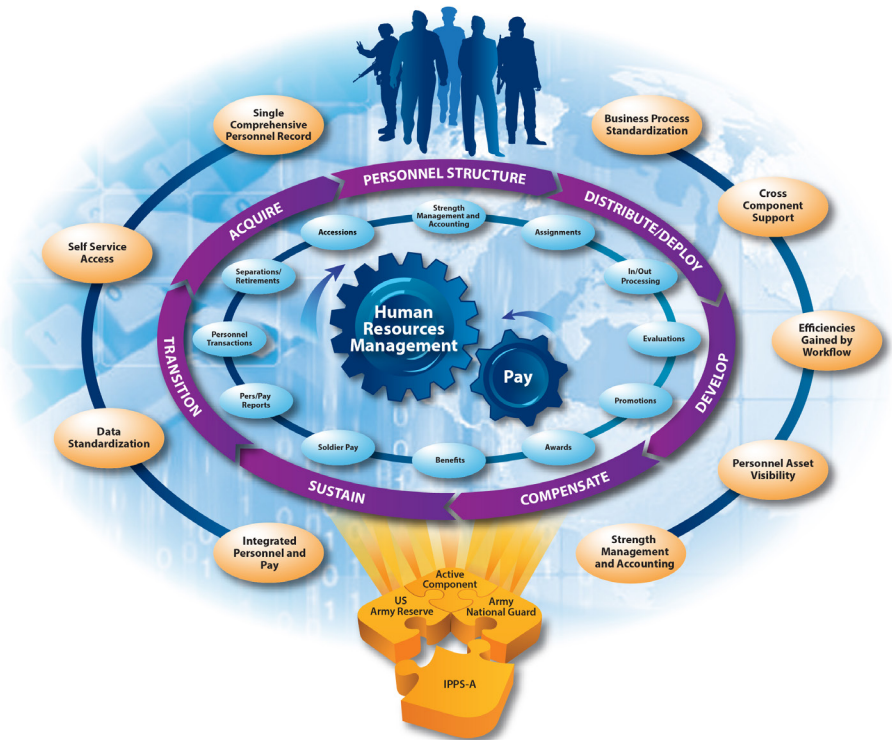# Integrated Personnel and Pay System – Army (IPPS-A) Increment I

Executive Summary

- Integrated Personnel and Pay System – Army (IPPS-A) is a two increment program that streamlines Army Human Resources processes and enhances the efficiency and accuracy of Army personnel and pay procedures to support Soldiers and their families. Through a three phased delivery approach, Increment I of the IPPS-A program provides the foundational data for a single, integrated military personnel and pay system for all three Army components: the active-duty Army, the Army Reserve National Guard, and the Army Reserve.
- The Army Test and Evaluation Command (ATEC) conducted a two-part FOT&E event from March 2014 through January 2015 in accordance with an ATEC-approved test plan.
- IPPS-A, as it exists in Increment I, is effective and suitable. IPPS-A is survivable against an outsider cyber threat. The capabilities available in this increment are limited; the program should continue to improve IPPS-A in order to deliver the full set of necessary capabilities.
- The IPPS-A Increment I system demonstrated the capability to produce its primary product, a Soldier's Record Brief (SRB), which is a single, integrated compilation of personnel and pay data collected from various, external authoritative sources.

System

- IPPS-A is a two increment program that streamlines Army Human Resources processes and enhances the efficiency and accuracy of Army personnel and pay procedures to support Soldiers and their families. Increment I interfaces with legacy applications to create a trusted, foundational database. All authoritative data remain in the legacy systems for Increment I. Increment II will become the authoritative data source as the necessary functionality of the legacy systems to be subsumed is incorporated.
- IPPS-A is a web-based tool, available 24 hours a day, accessible to Soldiers, Human Resources professionals, Combatant Commanders, personnel and pay managers, and other authorized users throughout the Army. The Army intends for IPPS-A to improve the delivery of military personnel and pay services and provide internal controls and audit procedures to prevent erroneous payments and loss of funds.

- IPPS-A interfaces with 15 other Army and DOD systems to acquire personnel and pay data, which it integrates into a single record for each Soldier. These systems include the Defense Enrollment Eligibility Reporting System – Personnel Data Repository, Electronic Military Personnel Office, Standard Installation and Division Personnel Reporting System – Guard, and Total Army Personnel Data Base – Reserve. IPPS-A's SRB acts as a trusted, but non authoritative, display of data contained in the various external systems; any changes required to the data must be made within the existing 15 Army and DOD personnel systems and cannot be accomplished within IPPS-A. The SRB displays a Soldier's military career personal information, qualification skills, training, assignment history, and various other Soldier attributes.

Mission

Commanders will employ IPPS-A as a comprehensive system for accountability and information to support command decisions regardless of component or geographic location. Army components will use IPPS-A to manage their members across

the full operational spectrum during peacetime, war, through mobilization and demobilization, capturing timely and accurate data throughout. Soldiers will use IPPS-A as a single, integrated personnel and pay system that will provide personnel and pay management functionality for all Army components.

Major Contractor
Increment I: EDC Consulting LLC – McLean, Virginia

Activity

- ATEC conducted a risk assessment of IPPS-A Increment I on June 19, 2014, in accordance with DOT&E Information and Business Systems Policy. Due to the low risk of the capabilities being delivered in Increment I, the risk assessment allowed for the delegation of test plan approval to ATEC.
- ATEC conducted an FOT&E event from March 2014 through January 2015. The FOT&E was conducted in two phases.
  - Phase 1 of the FOT&E utilized email surveys of a sample of the worldwide Army population including Active, Army National Guard, and Army Reserve personnel.
  - Phase 2 included specific test actions at Rock Island Arsenal, Illinois, and Camp Shelby, Missouri, in January 2015.
- In November 2014, ATEC conducted a cybersecurity assessment on IPPS-A Increment I; however, the test had several limitations. In April 2015, ATEC conducted a second cybersecurity assessment, which had fewer limitations. During these cybersecurity assessments, the Army's Threat Systems Management Office (TSMO) conducted operations remotely from Redstone Arsenal in Huntsville, Alabama, and onsite at the Human Resources Command in Fort Knox, Kentucky, and Acquisition, Logistics, and Technology Enterprise System and Services in Radford, Virginia. Testing was conducted in accordance with the DOT&E Information Assurance policy.
- DOT&E submitted a classified FOT&E report in April 2015 and a classified cybersecurity report in October 2015 detailing the results of testing.

Assessment

- IPPS-A Increment I, as delivered, provides an SRB that is viewable through a web interface and can be printed out. Increment I does not provide the capability to add or edit personnel data. The ability to edit personnel and pay data will be phased in during the four releases in Increment II.
- The results of the online survey indicate the system was easy to use and the resources necessary to obtain and interpret the data on the SRB were adequate. The results also indicate that the training received and online resources available were sufficient for most Soldiers. Very few of the Soldiers used the help desk, and the associated survey results did not provide a significant response as to whether they were satisfied with the help desk support.
- The SRB can be categorized into 11 sections and the Header and Footer sections. Participants found data errors in all 11 sections and the Header and Footer sections of the SRB. Sections where more than 50 percent of the participants had

data errors include Personal/family data, Civilian Education, and Military Education. The FOT&E found that the legacy sources contributing to most errors are: Army Training Requirements and Resources System, Reserve Component Manpower System, and Standard Installation and Division Personnel Reporting System.
- During the FOT&E, as previously observed, data correctness continues to be a significant problem. Data displayed in the SRB, which is pulled from legacy Human Resources systems, have many problems, including missing and/or incorrect data. In addition, 93 percent of the Soldiers surveyed found errors in their records, as compared to the results from IOT&E in February 2014, where 95.2 percent of the Soldiers (181 of 190) found errors. This comparison shows the data correctness problem still exists and, as the sample size of users surveyed in the FOT&E is much larger (about 1 percent of the total Army military population) than in the IOT&E, the results are indicative of a widespread problem across the Active Duty Army, Army Reserve National Guard, and Army Reserve.
- The IPPS-A program manager does not have authority or mechanisms to correct data within legacy Human Resource systems. The IPPS-A Program Management Office and the Army G-1 are conducting a data correctness campaign that administers online surveys to facilitate reporting and resolution of data correctness issues. FOT&E results demonstrate that the Army is continuing to correct the data once a Soldier identifies an error and proactively initiates an action to get it corrected. However, the process is lengthy and difficult to fully accomplish due to legacy system limitations and documentation requirements.
- ATEC conducted a cybersecurity assessment of the fully deployed database in November 2014 using the Army's TSMO to portray the cyber threat. TSMO conducted operations remotely from Redstone Arsenal in Huntsville, Alabama, and onsite at the Human Resources Command in Fort Knox, Kentucky, and Acquisition Logistics and Technology Enterprise System and Services in Radford, Virginia.
  - The cybersecurity threat was not fully realistic due to limitations on time and rules of engagement at the Human Resources Command, Fort Knox, Kentucky. ATEC successfully completed a verification of fixes event addressing most of the findings on January 16, 2015. A follow-up cybersecurity assessment was conducted in April 2015.

- The follow-up cybersecurity assessment was found to be threat-representative. Testing uncovered areas that need survivability improvement. This will require the data centers to work with cyber defenders to improve detection capabilities, ensuring IPPS-A and interfacing systems are following Personally Identifiable Information (PII) encryption policies and performing periodic Cooperative Vulnerability and Penetration Assessments and cybersecurity assessments at the data centers hosting IPPS-A.
- The details of the cybersecurity test findings can be found in DOT&E's classified cybersecurity report dated October 2015.

Recommendations
- Status of Previous Recommendations. The Army is making satisfactory progress in the previous FY14 recommendations.

- FY15 Recommendations. The Army should:
  1. Continue to monitor data correctness with the Army G-1 to ensure IPPS-A will have accurate data to facilitate accurate transactions in Increment II.
  2. Conduct a fully threat-representative cybersecurity assessment for IPPS-A Increment I.
  3. Verify vulnerabilities identified in the threat-representative cybersecurity assessment conducted in April 2015 have been mitigated in order to maintain the performance and integrity of the currently operating system.
     - Work with cyber defenders to improve cyber detection capabilities.
     - Ensure all PII encryption policies are followed.
     - Perform periodic Cooperative Vulnerability and Penetration Assessments and cybersecurity assessments at the data centers hosting IPPS-A.