U.S.ARMY

US ARMY PEO EIS
PEO Enterprise Information Systems

the COMMUNICATOR

MAY 2019

EDITOR Ellen Summey | DESIGNER Racquel Lockett-Finch
For submissions contact, 703-806-3584, ellen.c.summey.ctr@mail.mil

PEO EIS PMs participate in 2019 Army IT Day

BY ASHLEY TOLBERT, PEO EIS STRATEGIC COMMUNICATION DIRECTORATE

PEO EIS live streamed the PM panel and small business panel discussions at AFCEA NOVA Army IT Day. (U.S. Army photo by. Susan McGovern, PEO EIS Strategic Communication Directorate)

PEO EIS participated in the 18th annual Army IT Day in Chantilly, Virginia, on May 1. Deputy CIO/G-6 Mr. Greg Garcia and ASA(ALT) Principal Military Deputy Lt. Gen. Paul Ostrowski kicked off the morning program, which was followed by an afternoon panel of PEO EIS program managers (PMs) moderated by former Assistant Secretary of Defense (Acquisition) Hon. Katrina McFarland. The panel featured Col. RJ Mikesh, PM Army Enterprise Systems Integration Program (AESIP); Col. Chad Harris, PM Defensive Cyber Operations (DCO); Col. Enrique Costas, PM Defense Communications and Army Transmission Systems (DCATS); Col. Darby McNulty, PM Integrated Personnel and Pay System - Army (IPPS-A); Mr. Tom Neff, PM Enterprise Services (ES); and Ms. Balinda Moreland, Technical Chief, PM General Fund Enterprise Business System (GFEBS).

Mikesh spoke about the importance of data management for Army leaders, and the need for faster reporting. "It's all about the data," Mikesh said. "I am looking for industry to come talk to me about data management." In today's technical environment "you need to have real-time information reporting. That's what Army leaders are expecting of us."

...you need to have real-time information reporting. That's what Army leaders are expecting of us.

The PMs and Enterprise Solutions Director Stacy Watson participated in a speed networking session and met with an average of 14 companies per PM during the session.

The event hosted more than 600 attendees, with industry representatives from over 270 companies. The theme of this year's program was "Network Enabling in a Dynamic Environment," and the event was created to encourage collaboration and networking between Army leaders and industry.

Both the PEO EIS PM panel and the small business panel were recorded live, and the videos are available at: www.facebook.com/pg/peo.eis/videos.

Real-time access to human resources information huge benefit for VAARNG

BY JUSTIN CREECH, IPPS-A STRATEGIC COMMUNICATIONS

Chief Warrant Officer 2 Lionel Blair, systems information branch chief for the VAARNG and Sgt. 1st Class Cliff Klaye, senior financial manager discuss the IPPS-A during a senior leader engagement at Fort Pickett, Virginia, April 8-12. (U.S. Army photo by Justin Creech, IPPS-A)

The Integrated Personnel and Pay System – Army (IPPS-A), went live for the Virginia Army National Guard (VAARNG) on April 5, 2019. Soldiers and Commanders having real-time access to theirs and other Soldiers' information is already proving a benefit of the system, according to Chief Warrant Officer 2 Lionel Blair, systems information branch chief for the VAARNG.

"Commanders and managers being able to see their unit's information in real time is super powerful," said Blair. "They can see deployment stuff like readiness scorecards and duty statuses. Honestly, they can see the overall readiness of their unit in real time without depending on contacting a human resources (HR) professional."

The VAARNG has spent two years preparing to implement the IPPS-A system. IPPS-A is the Army's new comprehensive human resources system that has subsumed the Standard Installation and Division Personnel Reporting System (SIDPERS). The new system gives access to personnel records for every Soldier in the VAARNG, which means an increase in the number of Soldiers who need to know how to use the system. Blair said he and his team are working to help Soldiers get accustomed to IPPS-A.

"This system is more robust than SIDPERS," said Blair. "SIDPERS was binary, so only select people had access. Now, we've got 300 HR professionals in the system, plus commanders, 1st Sergeants and Sergeants Major. So, a lot of people are trying to get their footing and figure out their role in the system."

The reduction in systems, plus speedier uploading of new information is a benefit HR specialists have noted, according to Blair.

"They've seen orders go into IPERMS in a matter of seconds rather than having to manually upload them," said Blair. "That's definitely a positive of the new system."

Prior to having IPPS-A, HR specialists did not have a lot of contact with Soldiers. They would communicate with one another via email, or a quick phone call when a Soldier needed information. However, IPPS-A has created what Blair refers to as a ticket system, which he feels will force HR specialists and Soldiers to deal more directly with one another to solve an issue.

"The ticket system increases what I call touch time," said Blair. "If a Soldier asks me a question via the ticket system, I must open the ticket, read the comment, research something in another system, come back and answer question, then work a solution. That's holistic HR management which is a good thing. It increases visibility on the work we are doing as HR professionals."

Another benefit of IPPS-A is the Soldier's ability to update their profiles on their own without the need of a government computer. Now, Soldiers can be anywhere in the world and update their IPPS-A profile, which reduces delays that existed with prior systems.

Commanders and managers being able to see their unit's information in real time is super powerful.

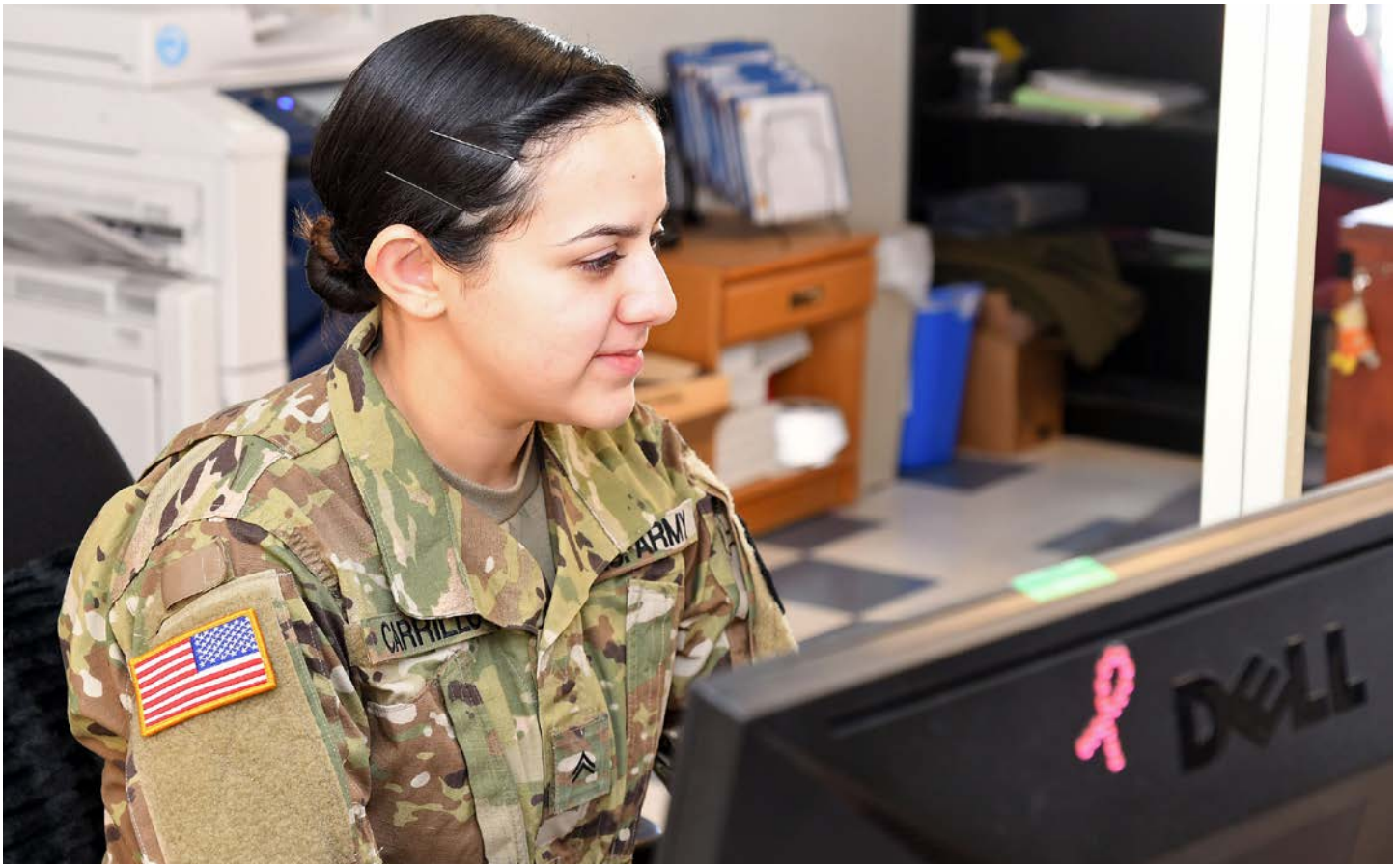
"Our Soldiers who are only here on drill weekend will especially benefit from this system," said Blair. "So, knowing if they get married they can submit their documentation on their own. They can do that in real time instead of waiting 30 days to submit a document. Before IPPS-A, Soldiers couldn't update their records on their own."

Blair and his team are already seeing the benefits of IPPS-A, which is particularly satisfying after going through such a long migration process.

"Getting to an end state of something we've been working on and seeing benefits is very satisfying," said Blair. "Now, we're shifting gears to training to make sure we're training the field users of the system. It's nice to be at this point."

Army considers additional multi-factor authentication measures

BY DEVON L. SUITS, ARMY NEWS SERVICE



Cpl. Ivanska Carrillo, a human resources specialist, goes through schedules on her work computer during unit mobilization and demobilization processes at Fort Bliss, Texas, Oct. 31, 2018. The Army is looking into additional authentication measures to improve the security of information-technology systems while providing more options to access Army resources online. Carrillo is assigned to the 210th Regional Support Group, Aguadilla, Puerto Rico. (U.S. Army photo by Sgt. Christopher A. Hernandez)

The Army is working on additional authentication measures to provide more options to access Army online resources while maintaining the security of information-technology systems. Army CIO/G-6 officials are working with Program Executive Office Enterprise Information Systems (PEO EIS) to consider alternatives to the Army's current multi-factor authentication process, or MFA. MFA requires users to prove their identity by presenting at least two points of verification across three major categories: something you know, something you have, and something you are, officials said.

"The commercial industry has seen that there's a greater need for protection, making sure the right people are accessing the right accounts," said Thaddeus Underwood, Identity Management and Communications Security division chief. "It makes sense that the Army is moving in the same direction. We are better protecting access to our IT networks to improve our cybersecurity posture by replacing username and password logins across the Army with MFA-secured options." Current MFA measures force Soldiers to use their Common Access Card and personal identification number to log into a government computer system, Underwood said. However, with a percentage of the Army currently serving in the Reserve or National Guard,

We are better protecting access to our IT networks to improve our cybersecurity posture by replacing username and password logins across the Army with MFA-secured options.

(continued)

some Soldiers don't have consistent access to government computer systems. "You've got Reserve and National Guard members who only come to a government facility on the weekend for their drill training," Underwood said. "If there is online training that they need to do … they could potentially do that from home if they have a CAC and CAC reader," he said. "How do we provide them that level of access without having to use a CAC?"

The Army is considering two MFA alternatives: an authentication-type application that Soldiers can download to their mobile device, Underwood said, and a pre-registered USB-type device, known as a Yubikey.

PHONE APP

The Army is looking into an authentication-type app to provide Soldiers access to official sites, without having to use a CAC and reader. In theory, Soldiers will download the app to their smartphone and register their device online, linking it to their Army identity, Underwood said. Once the app is registered, Soldiers will then log into official Army websites with their username and password. The site will trigger an MFA process and send a one-time-use passcode to the app on their device. After entering the passcode into the website, the Soldier will be authenticated to the site. The MFA process will provide access to personnel records, online training, and other applications without the need of a CAC-enabled computer. "We are at the final stages of developing the requirements. Next, we are going to ask commercial vendors to provide solution options," Underwood said. "We expect to have an initial-app prototype by this fall."

We are at the final stages of developing the requirements. Next, we are going to ask commercial vendors to provide solution options.

YUBIKEY

In addition to developing an app, PEO EIS is providing Yubikeys as an alternative option for MFA. A Yubikey is a registered USB-type device that can be inserted into a computer's USB port, like a self-contained CAC and CAC reader. The device serves as a second form of authentication after the user logs into an official website using username and password, Underwood said.

"The Yubikey solves the problem of not having a CAC and reader, but it doesn't solve needing a physical piece of equipment," Underwood said. "This device will probably be a better solution for some of our mission partners such as the American Red Cross, and first responders that act when an incident happens…and don't have a CAC to get access to our resources," he added. Yubikeys are currently going through integration testing by PEO EIS, Underwood said.

"Anytime you have new technology, you want to introduce it to existing technology and make sure that it will work," he said. "We expect user testing and field testing to begin in May."

MAY 2019

SUN	MON	TUE	WED	THUR	FRI	SAT
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

UPCOMING EVENTS

13 MAY: GFEBS-SA Assumption of Charter

14-16 MAY: TechNet Cyber

22 MAY: Forge Ribbon Cutting

22-23 MAY: NDIA 12th Annual Midwest Government Contracting Symposium

24 MAY: AUSA GW Chapter Luncheon

27 MAY: Memorial Day

29 MAY: AFCEA Belvoir Scholarship Presentation

29-30 MAY: PEO EIS Cyber Security Summit

30 MAY: PEO EIS Lunch & Learn

ASIAN AMERICAN PACIFIC ISLANDER HERITAGE MONTH • MAY

UNITE OUR MISSION

BY ENGAGING EACH OTHER

Army leaders look to industry for "transformation" of enterprise IT

BY ELLEN SUMMEY, PEO EIS, STRATEGIC COMMUNICATIONS DIRECTORATE

ARCYBER Commanding General, Lt. Gen. Stephen Fogarty, delivered the keynote address at the EITaaS collaboration day on May 7, 2019. ((U.S. Army photo by Cecilia Tueros, PEO EIS Strategic Communication Directorate)

FORT BELVOIR, Va. — The Army is conducting a pilot to transform the way it provides enterprise information technology (IT) at its installations. This initiative, called Enterprise IT as a Service (EITaaS), is a cooperative effort between Army Cyber Command (ARCYBER), Army Contracting Command – New Jersey (ACC-NJ), Army Chief Information Officer (CIO)/G-6, and Program Executive Office Enterprise Information Systems (PEO EIS). EITaaS is a departure from the Army's current, government-owned and operated approach to enterprise IT delivery, and looks to industry to provide a reliable, resilient and secure network. This effort is informed by similar pilots conducted by both interagency and joint service partners.

Kicking off the pilot process, PEO EIS hosted an EITaaS government/industry collaboration day at Fort Belvoir, Virginia, on May 7, 2019. The event garnered a high level of interest among industry, prompting organizers to add a second session to accommodate the nearly 400 registered attendees.

In his keynote address, ARCYBER Commanding General, Lt. Gen. Stephen Fogarty, spoke about the Army's intent for the EITaaS initiative and solicited candid feedback from industry. "What we want to do is make a dramatic improvement in the network and IT capabilities that we're providing the Army, and we want to be able to do it at a fair cost, we want to do it really according to industry standards," Fogarty said. "(W)e've got to work with industry to help define what those potential methods of delivery could be."

Fogarty told attendees that Army leaders were looking for "transformational" approaches to enterprise IT delivery, and stressed that all options were on the table. "For us, this really is a transformation of the way we're looking at the network, the way we think we can solve this very tough, very important problem for the Army," Fogarty said.

The EITaaS pilot will initially focus on Army Futures Command headquarters in Austin, Texas, and Fogarty said the effort could expand to two additional locations in fiscal year 2019. "There is potential for two additional pilots this fiscal year, so for us the ability to take the lessons learned from this process and see how fast we can turn additional pilots, will be critically important," Fogarty said.

To deliver this prototype solution, the Army is considering the Other Transaction Authority (OTA) under 10 USC 2371b, which allows the Department of Defense to shortcut the traditional acquisition process for certain prototype and pilot projects. Chris Fotiadis, an agreements officer from ACC-NJ, spoke about prototype OTA agreements, and the requirements to use them. "In order to qualify for an OTA project, you have to meet three really critical criteria," Fotiadis said. The project must be defined as a prototype, it must directly enhance mission effectiveness, and it must have significant non-traditional defense contractor participation (or 1/3 cost sharing by traditional defense contractors).

Col. Kevin Litwhiler, deputy commander of Digital Integration, Network Enterprise Technology Command (NETCOM), explained the draft acquisition approach and highlighted areas where the Army is seeking input from industry. Among other questions, Litwhiler asked how industry representatives would restructure the EITaaS lines of effort, and which DoD or Army policies they might recommend replacing with commercial standards. "Policies can change," Litwhiler said. "We need you all to advise us of what you think is the barrier to entry, what is going to cause you some challenges, so we can understand what we need to look at with the new technologies, and what is an equivalency to our current policies and current structure," so they can be updated if needed.

Dan Joyce, assistant PEO for Networks, Cyber and Services at PEO EIS, said the prototype proposal opportunity notice is tentatively scheduled for publication on June 5. For more information on the EITaaS pilot sources sought notice, search solicitation number W15QKN-19-X-05Z1 on fbo.gov. All presentation slides from the event are available at: https://www.fbo.gov/utils/view?id=ac5685d7a87e45c20585c1e379feb72e.

Mr. Ronald W. Pontius, Deputy to the Commanding General, U.S. Army Cyber Command, speaks at the 2019 AFCEA NOVA Army IT Day, May 1, 2019. (Courtesy photo by AFCEA NOVA)

Lt. Col. Rob Wolfe, director of the PEO EIS Strategic Initiatives Group, participates in an interview with Defense Acquisition University professor Brian Yoo on May 3, 2019. (U.S. Army photo by Ellen Summey, PEO EIS Strategic Communication Directorate)

Lt. Gen. Paul Ostrowski, ASA(ALT) principal military deputy, speaks about the Army's commitment to modernization at the 2019 AFCEA NOVA Army IT Day, May 1, 2019. (Courtesy photo by ASA(ALT))

Nearly 400 industry representatives attend the Enterprise IT as a Service collaboration day at Fort Belvoir, Virginia on May 7, 2019. (U.S. Army photo by Cecilia Tueros, PEO EIS Strategic Communication Directorate)

Former Assistant Secretary of Defense (Acquisition), **Hon. Katrina McFarland**, hosted the PEO EIS PM panel discussion. (U.S. Army photo by Susan McGovern, PEO EIS Strategic Communication Directorate)

Acting Acquisition and Systems Management Director, **Michelle Walker** conducts a lunch and learn session about DoD Instruction 5000.75 on April 25, 2019. (U.S. Army photo by Cecilia Tueros, PEO EIS Strategic Communication Directorate)

EIS SNAPS