The Southeast Scoop

Southeast Regional Newsletter

April 2025

CURRENT EVENTS

- **5 MAY – 6 JUNE:** Rapid7 Nexpose Pilot
- **15 MAY:** CCB Meeting
- **16 MAY:** SIPR CONMON
- **20 – 22 MAY:** SCIP Class
- **26 MAY:** Memorial Day
- **28 MAY:** Regional IMO User Group Meeting
- **MAY:** OPSEC Awareness Month

NOTEWORTHY

- NEW interim process for account requests (baseline and above baseline) outlined HERE!
- Before ATCTS sunsets on **1 May 2025,** all users should download relevant training certificates, all DD2875's, DA7789s, appointment orders, IT user agreements, and other credentials from their ATCTS profile.
- ATCTS FAQs page HERE
- Find the ATCTS click sheet here and Account Validation System (AVS) EXORD here
- Link Solutions employees of the month Victor Butler and Megan Felesky
- NEW! Southeast Region Policies document library published on the site visitor landing page linked HERE. V-Team leads, chiefs, and above may add policy documents for Army-wide read access. *Note that the rest of the RNEC SPO site is NOT largely accessible Army-wide.*

NEW! PLA DOCUMENT REPOSITORY

With the imminent sunset of ATCTS, an application has been developed to enable SE RNEC personnel with Privileged Level Access (PLA) to store required account documentation for operating as an administrator on the SE RNEC network.

Access the application, Power BI dashboard, and training videos HERE!

- One stop location for SE RNEC personnel to upload required PLA documents.
- Training videos are provided.
- Personnel can only submit and access their own records.
- Personnel can review their own documents uploaded through the app.
- Personnel can delete their own records.
- The submitted documents are fully accessible by the Accounts Management V-Team.
- A dashboard is included to enable leadership the ability to track submissions.

An additional process is in development to enable non-SE RNEC personnel requiring PLA access the opportunity to submit required account documentation.

NEWS FEEDBACK

Story Submissions, Comments, Dad Jokes, & Special Recognition Requests

Email us!

sernec_RegionalNews@army.mil

SOUTHEAST DAD JOKE CORNER

What is red and bad for your teeth?

A brick!

Submitted by Stephen Giza, SE Region Director

DID YOUR PRINTER MAKE THE CUT?

Is your Stewart/HAAF printer in Print Logic? If not, submit an AESMP ticket to get your printer added! Items highlighted red on this document have *not* been migrated. (User must be a member of the 93D_SE_RNEC_Trusted_Agents team to view the linked document.)

OPSEC AWARENESS MONTH - MAY 2025

May is the Army's OPSEC Awareness month so please take a few minutes to review. As a DOD Civilian, you have access to information that could be valuable to our adversaries. Practicing good OPSEC helps protect yourself, your colleagues, and ultimately the War Fighters mission, ensuring they are able to come home to their families, like you do, every night. Here are some best practices for some of the overlapping areas of our lives.

At Work:

- **Clean Desk Policy**: Clear your desk of sensitive information, including CUI, at the end of each day. Store CUI materials according to established procedures. Secure classified material in approved containers.
- **Visitor Control**: Escort all visitors and challenge anyone without proper identification. Control access to areas where CUI is stored or processed.
- **Social Engineering Awareness**: Be cautious of unsolicited phone calls, emails, or visitors seeking information. Verify identities and report suspicious activity.
- **Data Security**: Follow established procedures for handling sensitive data, including CUI. Use only authorized devices and software. Encrypt CUI when transmitted or stored electronically.
- **Physical Security**: Be aware of your surroundings and report suspicious activity. Secure your workspace and CUI materials when unattended.

At Home:

- **Social Media Caution**: Be mindful of what you share online. Avoid posting details about your work, travel plans, security measures, or anything related to CUI.
- **Trash Disposal**: Shred sensitive documents, including CUI, before discarding them.
- **Home Security**: Maintain good home security practices, including strong locks and alarm systems, to protect CUI if stored or accessed at home.
- **Conversations**: Be discreet when discussing work-related matters, including CUI, even with family and friends.

Online:

- **Strong Passwords**: Use unique, strong passwords for all accounts, especially those used to access CUI, and change them regularly.
- **Phishing Awareness**: Be wary of suspicious emails and links. Don't click on anything you don't trust. Report suspected phishing attempts.
- **Software Updates**: Keep your software and operating systems up to date to patch security vulnerabilities that could compromise CUI.
- **Privacy Settings**: Review and adjust your privacy settings on social media platforms.

In Public Places:

- **Conversations**: Avoid discussing work-related matters, especially anything involving CUI, in public places where you can be overheard.
- **Identification**: Be mindful of displaying your DOD affiliation in public.
- **Travel Awareness**: Be cautious when traveling, especially to foreign countries. Register with the Smart Traveler Enrollment Program (STEP). Be aware of CUI handling requirements while traveling.

For more information on Training (CEUs), Certification (C/OSINT) and Poor Practices of OPSEC reference the TRIFOLD linked HERE.

FORT JACKSON ENTERPRISE DIVISION TEAM

Front row from left to right: Alex Williamson (Hosting & Hoteling Customer Support System Administrator), Lilly Hatten (Hosting & Hoteling Sever Administrator), Lashanda Howard (Hosting & Hoteling Customer Support System Administrator), Timothy Strong (Hosting & Hoteling Customer Support System Administrator)

Back row from left to right: Edgardo Perez, (Hosting & Hoteling Customer Support System Administrator), Nicholas Floyd (Hosting & Hoteling Sever Administrator), and Derrick Taylor (Hosting & Hoteling Division Chief)