

JBLM NEC Information Assurance Division Newsletter

"The Honey Badger Gazette"

JBLM Network Enterprise Center
Amy Ridgeway, NEC Director
Dan Soderberg, NEC Deputy Director
Virginia Register, Chief, IA Division

Special points of interest:

- > IA Newsletter Introduction
- > PII
- > NEC IA Wireless Team
- > Check to ensure VPN Client works BEFORE going TDY.
- > UDCI-Have a process in place to quickly respond to Unauthorized Disclosure of Classified Information

WELCOME TO THE NEW JBLM NEC INFORMATION ASSURANCE (IA) DIVISION NEWSLETTER!

WELCOME TO THE NEW NETWORK ENTERPRISE CENTER (NEC) INFORMATION ASSURANCE (IA) NEWSLETTER!

The purpose of this newsletter is to provide information to our JBLM Community that enhances IA Awareness, share insights on best business practices, and stimulate discussions on security related topics to augment or improve security practices in support of the NEC's Mission and the Army's Information Assurance Program.

When your organization is looking at adding new software, hardware and any other new technology to the network, contact the NEC at the beginning of your project. Notifying us at the start, will give us time to do our homework and provide you the service you expect. Our goal is to provide the latest and most effective

information assurance services, security and business practices that best supports the JBLM Community.

As you read through this newsletter, please think of ways we can improve it so it is a valuable source of information for you and your team. Feel free to contact the NEC IA Division. See our Points of Contact listed in the newsletter.



Personally Identifiable Information (PII)



What is a PII?

PII is any information about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, and biometric records. This includes, but is not limited to, education records, financial transactions, medical files, criminal records, or employment history. This information can be in hard copy or electronic format, stored on personal computers, laptops, Blackberries, or in databases.

Reporting a PII Incident

PII data must be protected from breach or compromise. A PII breach or compromise occurs when it is suspected or confirmed that PII is lost, stolen, or otherwise available to individuals without a duty related official need to know. This includes, but is not limited to, posting PII on public-facing websites; sending PII via email to unauthorized recipients; providing hard copies to individuals without a need to know; loss of electronic devices or media storing PII; use by employees for unofficial business; and all other unauthorized access to PII. PII infractions must be reported within 24 hours of the discovery. To prevent sending PII ensure you encrypt the information when emailed, and send it only to individuals that have a need to know.

PII incident information is located at:

https://www.rcert-c.army.mil/PII/PII_index.htm

Inside this issue:

IA Points of Contact	2
VPN Client	2
UDCI	2

Network Enterprise Center
Information Assurance Division

Information Assurance Division

NEC IA Wireless Team

In accordance with BBP 09-EC-M-0010, para 5.A(5), Wireless Security Standards: The IA Division will monitor and administer a wireless intrusion protection system (WIPS) and conduct war driving. "War driving" is physically driving around JBLM and scanning for unauthorized wireless gateways and Access Points (APs) on the JBLM Network. Once identified, these rogue devices will be disconnected and/or blocked from the network. NEC is responsible for monitoring, maintaining and administering a WIPS. The NEC IA Wireless Team will be visiting your building soon!

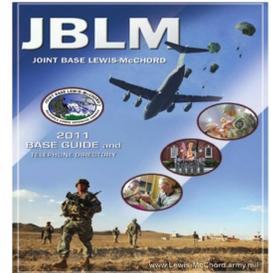
VPN Client

A Virtual Private Network (VPN) is a private data network that makes use of the remote access service, maintaining privacy through the use of a tunneling protocol and security procedures. VPN Client software gives the JBLM community access to this data network while out on TDY.

Check your VPN Client to ensure it works BEFORE going TDY. Work with your IASO/IMO to ensure everything is configured properly and the right certificates are installed. You can make your TDY a lot easier!

JBLM NEC

JBLM NEC
Bldg 4174
4174 Kaufman Avenue
JBLM, WA 98433



We're on the web!

<https://ft.lewis.army.mil/IA/>

Come join us in the IA Forum! (Restricted to IASOs and IAMs, and must be invited).

<https://www.milsuite.mil/book/groups/jblm-community-ia-forum?>

IA Division Points of Contacts

NEC Incident Handling Team Email:

JBLMNETCOMNECIncidentResponse@conus.army.mil

IA Reference Material

More detailed Information Assurance information can be found in these references:

AR 25-2, Army Regulation on Information Assurance.

BBP on Classified Information Spillage Requirements: See BBP 03-VI-D-001
https://www.milsuite.mil/wiki/Best_Business_Practices

What is a UDCI?

UDCIs can

- *Jeopardize our soldiers living in combat
- *Compromise or cause grave damage to the security of our nation
- *Provide information to unauthorized sources

What is a UDCI? A UDCI is an Unauthorized Disclosure of Classified Information. A UDCI is a security incident that results in the transfer of Classified information from a system with higher classification to a system with lower classification.

When working with classified information you must be careful. Most classified spillages occur due to user negligence.

If you are unsure of the information classification you are about to send via email, post in a slide presentation, send in a report, check with your security manager BEFORE you send it. This is especially true for those documents you did not create, but are copying and reusing. If you did not create it, check it! Open all files you receive on CDs, DVDs and other portable media on a standalone computer and inspect every page for Classified markings on documents, in front of paragraphs, embedded in pictures and PowerPoint presentations.

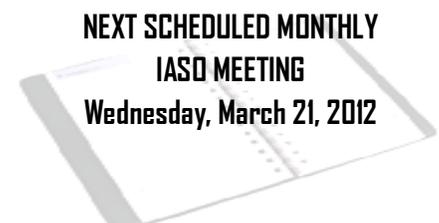
If you didn't produce it - you **MUST** inspect it. Only open e-mail attachments from **known** sources. If you are unfortunate

enough to have a UDCI, have a response plan in place to contain, clean up, and restore systems and services. Each classified spillage costs your organization and the NEC time and money to clean up. Preventing classified spillages starts with **YOU!**

Contact the NEC Incident Handling Team if you have a spillage or any questions.

DPTMS also has monthly **Classification Marking Courses**, Intranet Website (Fort Lewis Only):

<https://ft.lewis.army.mil/coisec/SEAT.htm>



**NEXT SCHEDULED MONTHLY
IASO MEETING
Wednesday, March 21, 2012**

Articles coming in next issue:

Got any ideas for articles you would like to see in the IA Newsletter? Let us know!

Please send suggestions to
JBLMNETCOMNECIncidentResponse@conus.army.mil