Transcript: Cybersecurity Part 3

Welcome to this ALMR training series on cybersecurity. This presentation will focus on end user cyber security and best practices.

As we discussed in Part 2 of this series, the AMLR network is managed using the highest level of Department of Defense Security standards. The AMLR system has procedures in place for cyber security practices, both at the system management level and at the user level. It is important to note that ALMR users that interact with the equipment on a daily basis may be the first to notice any potential cyber security issue or other malfunction.

Because of the interconnected world that we live in, and the multiple systems that most of our users are interacting with each day, several different security requirements and best practices are recommended for all users, especially those that have access to equipment that is directly connected to the ALMR network such as users in dispatch centers, users that can access key management facilities, management consoles, and others.

Procedure 200-5 in the ALMR policies and procedures outlines training requirements and other cyber security requirements for all of our staff. This presentation will outline some brief recommendations for all users. As a reminder, we recommend you take the annual security training offered by the DoD outlined in that procedure. If you are required to take that training as part of your job and access, be sure you complete the training requirements annually as a refresher.

In general, users should be sure to maintain the physical security of equipment. Remember that criminal justice information system rules are in effect for all ALMR equipment and similar equipment that you may have in your facilities. These rules include that uncleared personnel must have an escort when accessing physical equipment. Users should also ensure that maintenance work or other types of scheduled outages, or requests for information are being performed by authorized staff for an authorized purpose. If you have questions about ALMR specific equipment, you may always contact the help desk to ensure that a request that you are being asked to do or for downtime is being scheduled as legitimate.

Make sure that USB or other removable media is never connected to any type of equipment and don't provide access to equipment to unknown persons that may request it via phone or e-mail. Keep in mind that you may always contact your local IT department or the help desk to verify any potential emails that request you to perform actions. These types of

attempts are common to allow unauthorized or malicious actors to gain access to equipment, to be able to install software, gather information, or perform other functions.

If equipment in your facility is connected to the Internet, there are additional measures that must take place to ensure that there is not any potential malicious software or actions that can take place via your Internet connection. Keep in mind that ALMR equipment is not connected to the Internet, however other equipment that is connected can be compromised using malicious software. The most common way that equipment is compromised is by clicking on unknown links in emails or on websites. This may put tracking cookies or any type of unauthorized software that could result in information being stolen or the equipment being held for ransom via encryption, otherwise known as ransomware.

Be sure to not click on any unknown links or emails. If a known website is referenced in an e-mail, it is better to directly type in the address of the site rather than clicking to a link which may redirect you to a similar site but one that's impersonating the legitimate one. Keep in mind that emails are generally formatted to look like legitimate communications. This could be occurring in your personal world, such from your bank or another association, or could be formatted to look like people in your organization.

If you are receiving information requests or actions to do something. Make sure that you follow your company policy and procedures. We have seen increases in emails coming from people such as managers or others that you may know within your organization to do a task, connect with information, call a phone number, and other items. You may even see comments such as that person is in a meeting and unavailable by phone, but this task needs to be performed quickly.

These are all phishing attempts in order to gain information that can be used as ransomware or to obtain system access. In our personal lives, oftentimes this may be used to send money or give unauthorized access to banking or personal information. In your professional world, this could expose access to public safety data and other sensitive information. Make sure that any emails you get, even if it's purporting to come from your supervisor, IT department or the ALMR help desk, is verified. Call the correct point of contact via phone to verify it before giving any information that you're unsure of.

If you see a computer, workstation or other piece of equipment acting in ways that are unexpected, also notify your IT department immediately as this could be a sign of a potential cyber-attack or potential issue from malicious software. If you're encountering this odd behavior in workstations or computer terminals, know the procedure to immediately report issues to your IT department at your local site, both during normal

business hours and after hours. You may have a security manager or other points of contact that may be able to assist you and make sure you know the protocols for taking action.

Sometimes these protocols can include actions such as disconnecting that computer or station immediately from the network, usually by physically unplugging a network or ethernet cable from the computer or perhaps turning off the Wi-Fi function the system is using. This can help save information if the system is actively being encrypted.

If there are any odd behavior for ALMR connected equipment such as dispatch consoles or others, contact the ALMR help desk 24/7. You can do this by contacting the ALMR main number and following the prompts for after-hours access.

Additional best practices, including applying operating system software patches regularly. For some IT departments, this patching may be managed for you and may be installed through an automatic or batched process. If it is not and you are prompted to install updates, especially those updates that are for security purposes, be sure you apply those patches regularly to ensure your computer is maintained as safe as possible.

ALMR connected computers such as dispatch consoles need to be rebooted to allow patches to install properly. Be sure to reboot systems on a regular basis to allow those patches to install.

Password management is one of the simplest and easiest tasks that each one of us can undertake to keep our system safe and secure. Make sure your passwords are changed frequently and that they're complex. Use letters, numbers and symbols, but not dictionary words. Make sure that you do not reuse passwords. Passwords on various websites can be compromised due to data breaches and other incidents, and those passwords will then be used to access other sites. For example, you would never want to use the same password for a streaming service as you might use for your bank or for another critical piece of information.

Make sure when receiving information via e-mail or text that you are questioning it, especially when it's unsolicited or unusual. Verify via phone with the sender that the information they are asking for is legitimate.

Finally, be sure not to plug in any unauthorized devices to computers or other sensitive equipment at the workplace. This can include plugging in mobile phones via USB connection to charge. Never plug in anything via USB to any sensitive piece of equipment. Your IT department may have disabled this function or have other restrictions related to removable media. Always plug personal devices into charging power outlets only as data

can be compromised via that USB cable, even if only used for charging. Make sure only authorized devices by your IT department are allowed into your network at all times. These simple best practices will take care of the majority of potential methods of entry for malicious actors intent on gaining access to systems or causing other malicious actions.

Don't hesitate to reach out to the ALMR help desk or operations management office for any questions on cyber security or other add matters related to the ALMR system. You can access the help desk 24/7 in an emergency by dialing the number on the screen and follow. The prompts to reach an after-hours technologist.