



**FOR IMMEDIATE RELEASE**

**March 1, 2018**

018-018

By Capt. Joseph Siemendel

### **Cyber Hygiene: Alaska National Guard hones in on efficient cyber security during Arctic Eagle 2018**

**JOINT BASE ELMENDORF-RICHARDSON, Alaska** — An electronic sensor on the more than 800-mile stretch of the Trans-Alaska Pipeline System was just triggered. A potential leak is happening, so you send a team out to respond. When the team shows up, it was a false alarm, but then another alarm goes off, then another, and before you know it every sensor is chiming.

This scenario is very real, and all it takes is one malicious cyber attacker to make it happen.

As part of Arctic Eagle 2018, Alaska National Guardsmen trained on how to identify a potential cyber threat.

“We wanted to test what the operational impacts would be if this happened,” said Scott Moreland, exercise planner, Arctic Eagle 2018. “This will test the Guard’s ability to identify when it has happened and make sure it is being communicated.”

Arctic Eagle 2018 was an optimal time to conduct such a scenario. More than 1,100 Guardsmen from multiple states came to Alaska to participate in the multi-facet exercise.

Multiple cyber based scenarios were part of the exercise. The first being a satellite crash and practicing cyber hygiene, followed by exercises on cyber security and cyber protection.

“We don’t currently have a real world cyber security mission, so what we presently do is called cyber hygiene, which is focused on training, awareness and outreach,” said Capt. Robert Gordon, Director of Computers and Communications, Alaska National Guard. “If a threat actor, wanted to know what the National Guard is doing, they can track that through their social media,” he said. “That is where cyber hygiene can help stop the attackers.”

Not having an extensive cyber program, and facing real world scenarios during an exercise, allows the Alaska National Guard to train and grow their program, and they called for assistance from other state National Guards to help.

Lt. Col. Thomas Pries, Director of Space and Integrated Air Defense, Washington Military Department, made the trip from Washington State to discuss the work being done in his home state in the cyber security domain.

“We have done some extensive work supporting public utilities districts in Washington state,” said Pries. “The knowledge of our National Guard cyber professionals is invaluable, and has already assisted in strengthening security of the networks our citizens rely on every day.”

Another part of Arctic Eagle 2018’s cyber exercise was to identify a phishing attack on the city of Valdez, mainly targeting the shipping port. The Port of Valdez handles more than 1.5 million barrels of crude oil, along with other goods annually.

“We chose the port because we wanted to know how much it could possibly disrupt the operations, and what actions would take place, mainly communicating with other organizations about the phishing attack,” said Moreland.

Starting to have those kinds of conversations, according to Moreland, was a priority during the exercise.

“We want to know if the message is getting out, so as one attack happens, then another, then another, were the other organizations warned, communication is critical when it comes to getting in front of mysterious disrupters,” said Moreland. “One of the goals of Arctic Eagle 2018 was to have scenarios that included security and protection of critical infrastructure, we feel like including cyber in the exercise meets the state’s intent.”

###

## PHOTOS

1. **Attached pdf** includes story and a small selection of low-resolution photos for viewing on screen.
2. **Flickr link** includes an event album with the complete selection of full-resolution, free downloadable images. (May not be accessible from all military computers.) <https://www.flickr.com/photos/alaskanationalguard/albums/72157692971310344>
3. **DVIDS link** includes story and selected full-resolution photos. (Primarily for media, DVIDS is accessible from .mil computers.) <https://www.dvidshub.net/news/267647/cyber-hygiene-alaskan-national-guard-hones-efficient-cyber-security-during-arctic-eagle-2018>



### 180224-Z-ZA470-0004

Members of the Air and Army National Guard, along with DoD civilians and contractors, work alongside each other in the white cell, Feb. 24, 2018, Alaska National Guard Joint Force Headquarters, Joint Base Elmendorf-Richardson, during Exercise Arctic Eagle 2018. The white cell facilitates accurate simulation of complex scenarios during the exercise, and houses representatives from multiple government and non-government agencies. (U.S. Air National Guard photo by Senior Master Sgt. Paul Mann)



**180228-Z-PL215-0004**

Washington Air National Guard Lt. Col. Thomas Pries, director of operations, 262nd Cyber Operations Squadron, writes down information presented at a cyber brief on Joint Base Elmendorf-Richardson, Alaska, Feb. 27, 2018. This particular cyber brief was a part of Exercise Arctic Eagle 2018, a special focus exercise managed by the Alaska National Guard to test and validate Arctic capabilities, such as identifying cyber attacks throughout the state. (Alaska Army National Guard photo by Pfc. Grace Nechanicky)



**180228-Z-PL215-0007**

Richard Gloo, senior software engineer at Assured Information Security, Inc., gives a demonstration on cyber threats and how to recognize them to service members taking part in Exercise Arctic Eagle 2018, Joint Base Elmendorf-Richardson, Alaska, Feb. 27. The purpose of this training is to ensure service members can proficiently identify cyber threats in real-life scenarios, and can operate in a joint, interagency, intergovernmental and multinational environment. (Alaska Army National Guard photo by Pfc. Grace Nechanicky)