Press Release

Release No: 2411-02

November 5, 2024

Fort Drum Public Affairs

Fort Drum Public Works cyber and IT technicians practice infrastructure threat response

FORT DRUM, N.Y. -- Directorate of Public Works cybersecurity, information technology, and water system operation professionals combined their technical expertise to work through a “what if” crisis scenario Oct. 24 at Fort Drum.

Facilitated by representatives from the Department of Homeland Security’s Critical Infrastructure Security Agency, the tabletop exercise tested what this team would do if the installation’s water supply was compromised – first in the hours following the attack, and then the days after until they reach crisis resolution.

“The purpose of the exercise was to evaluate the garrison’s ability to respond to and recover from a cyber incident that impacted the water telemetry control system,” said Pete Owen, CISA protective security adviser. “Our objectives would be to identify any planning gaps, such as reporting requirements and service level agreements, and we want to identify capability shortfalls in resources.”

Owen said the exercise was developed as a “free-flowing discussion” where they could inject details, such as the revelation of an insider threat, while keeping the scenario authentic.

Tom Hudon, PW chief water operator, said the exercise helped to identify where they could make improvements in communication and documentation.

“Our priority is always going to be providing clean, safe water to the community,” he said.

Hudon said the automated water control system was built where daily checks can be conducted within a short amount of time, with minimal manpower requirements, and with redundancies in mind.

“If we had to shut the system down, we could still do everything manually for an extended time with just the people we have and there would be no interruption in service,” he said.

Robert Clements, Fort Drum information management officer, and April Eddy, Fort Drum information system security officer, coordinated the exercise for PW team members. An actual incident response would require coordination and input from multiple agencies and organizations, but Clements said the tabletop exercise focused on the technical aspect of an emergency response.

“We wanted to get the technical team together to walk the process through the roles of each member and how the work passes between those roles,” he said. “What Tom Hudon’s team does to protect the water system itself is different than what the system administrators and information system security officers do to protect the network. Putting everyone together helps to break down those silos between processes and streamlines our ability to respond to any type of IT incident.”

From what Eddy observed, she said the team managed to collect some lessons learned from the exercise, and now they can incorporate them into the response plan.

“This exercise takes in all of their expertise so that it is not just one person with all the knowledge,” she said. “Even if it didn’t always go smoothly, I’d say it was a win because we identified some shortfalls we can fix.”

Eddy said that the Directorate of Emergency Services and Directorate of Family and Morale, Welfare, and Recreation have recently had information technology evaluations, and that PW would require another for heating, ventilation and air conditioning (HVAC).

“There is a risk management framework requirement for each system to review the continuity of operations plan (COOP),” she said. “Each system within an organization – whether it’s CCTV, HVAC or water – has a COOP so that if the system crashes or something compromises it then you have a plan to bring it back up and functioning again.”

The Black Start exercise in 2023 tested the installation’s ability to recover from a massive power outage. Not only did the lights turn off, but automated systems were temporarily disabled. Hudon received the systems alert from his home and managed to get the water telemetry control system to return operations to normal. People might have been inconvenienced by the lack of lights, but there were no disruptions in their water supply.

“Information technology literally touches everything and every organization on post whether people realize it or not,” Eddy said. “It needs to be protected, and part of that protection is a plan to restore the system in case of a disruption or failure.”

###

Media with questions regarding this press release should contact Fort Drum Public Affairs, Katie Wright, 315-772-9043 or katherine.e.wright12.civ@army.mil

Photo Captions –

ITR1: Protecting Fort Drum’s water system from a cyberattack was the subject of a tabletop exercise in October involving Directorate of Public Works cybersecurity, information technology, and water system operation professionals. (Photo by Mike Strasser, Fort Drum Garrison Public Affairs)

ITR2: Tom Hudon, Fort Drum Public works chief water operator, and Stacy Bowen, cybersecurity specialist, were among the technical experts teaming up for a tabletop exercise Oct. 24 to test their organization’s response and recovery capabilities in a cyberattack scenario. (Photo by Mike Strasser, Fort Drum Garrison Public Affairs)