PCTC

Library Links

Martin O'Malley, Governor
Anthony G. Brown, Lt. Governor
Department of Public Safety and Correctional Services
Gary D. Maynard, Secretary
Police and Correctional Training Commissions
Charles W. Rapp, Executive Director

Volume 6, issue 3 | **December 6, 2011**

"If minds are truly alive they will seek out books, for books are the human race recounting its memorable experiences, confronting its problems, searching for solutions, drawing the blueprints of it futures."
~ Harry A. Overstreet

(Retrieved from http://www.useful-information.info/quotations/library_quotes.html#reading, accessed on 11/30/11)

Finding Funding…

If anyone is interested in finding out more about grants and available or likely-to-be-available funding for grants, check out www.grantsoffice.com/funded.aspx. The link will take you to the current issue of FUNDED, the online Grants Office Monthly Newsletter, as well as allow you to access back issues of the newsletter.

Brown Bag Lunch in the Library

Our next Brown Bag event is scheduled for January, and the next presenter in this series will be Dave Spikes. You'll be receiving an invitation very soon, and I hope you'll think about joining us for this session.

There have been four Brown Bag events thus far, and the feedback has been very positive. It's fun to have the chance to learn about something new in the course of the workday with no pressure or requirements.

So think about coming out for a session or two along the way; we've got lots more planned between now and the summer!

Acquiring New Materials

The library continues to add resources to its collection throughout the year. However, given budget constraints, the focus is currently on acquiring those items that are specific to a particular instructional or research need. Therefore, your input and recommendations are

critical to enhancing the quality and breadth of our library collection.

Please call me or send me items that may be of interest in the work you and those in your unit are involved in; ultimately this growth will benefit all of us here at the PSETC.

A Giveaway

There are extra copies of The Correctional Officer: A Practical Guide by Gary F. Cornelius (still shrink wrapped) in the library. If anyone is interested in having their very own copy, please let me know.

These will be held until just after the New Year.

Something New on the Shelf

It Can Happen Here, a DVD donated by Jennifer Beskid, has been added to our collection. This documentary was created to help inform school safety personnel on how to prepare for man-made and natural emergencies. Lessons learned from some of the most well-known acts of school violence are a major focus in this production as are the needed resources with which school safety plans can be either created or improved upon.

It's available for checkout to anyone who is interested (**DVD 371.7 ITC**).

Please read the following review which was written by Jennifer Beskid. Thanks go out to her for her time and input.

"It Can Happen Here," produced by the Weapons and Protective Systems Technology Center, the Applied Research Laboratory, and the Center for Community and Public Safety at The Pennsylvania State University, offers a compelling look at school shootings. The DVD focuses on the aftermath of three school tragedies: the Columbine (CO) shootings, the Platte Canyon (CO) hostage and shooting, and the Nickel Mines (PA) shootings.

The documentary features the principal of Columbine (at the time the shootings occurred), as well as the parents of a student injured in the shooting. It also features the parent of a girl who was killed in the Platte Canyon incident. First responders from Columbine, Platte Canyon, and Nickel Mines are interviewed throughout this DVD.

This documentary highlights support programs that have been established for students and staff to report suspicious activities as well as to reach out for help for themselves and/or their peers. It also speaks to how the police mentality has had to shift from one of public protection to one of threat elimination. Technological advances and resources are highlighted on the DVD. Overall, the DVD paints pictures of the aftermath of these school tragedies with very broad brush strokes. There is a human interest component of the DVD; however, very little information or resources are provided that would be new to most trainers in Maryland.

From the Headlines

***Hackers strike water-system controls in 2 states…**

Water utilities across the country are being urged to step up their cyber security in the wake of two incidents in which hackers gained access to computer systems that control pumps, pipes and reservoirs

By Shaun Waterman
The Washington Times

HOUSTON, Texas — Water utilities across the country are being urged to step up their cyber security in the wake of two incidents in which hackers gained access to computer systems that control pumps, pipes and reservoirs.

"We have alerted our members to these two possible incidents and advised them to monitor their [computer] systems and review their protection" procedures, Michael Arceneaux, deputy executive director of the Association of Metropolitan Water Authorities, told The Washington Times.

Federal officials said they were investigating, but downplayed the incidents, saying there was no evidence of a threat to public safety.

Earlier this month, the Illinois Statewide Terrorism and Intelligence Center reported a cyber attack on a small, rural water utility outside Springfield. Hackers, apparently based in Russia, gained access to the utility's computer systems and burned out a water pump by turning it on and off repeatedly, the center said in a bulletin dated Nov. 10. If the report is correct, it would the first cyber attack against U.S. infrastructure by foreign hackers.

On Friday, a hacker calling himself "Pr0f" posted screen shots from his computer showing him logged onto the control system of a water utility in the Texas town of South Houston. He said he had hacked the system to demonstrate the "insanely stupid" attitudes of federal officials who were playing down reports of the Springfield attack.

"I wouldn't even call this a hack," Pr0f wrote. "This required almost no skill and could be reproduced by a 2-year-old."

He said the control systems were easily accessible from the public Internet, but that he had not damaged them because "I don't really like mindless vandalism. It's stupid and silly."

In both the Illinois and Texas cases, the cyber attacks targeted special computerized equipment that remotely controls water pumps, pipelines and reservoirs. Such equipment, known as Supervisory Control and Data Acquisition (SCADA) systems or Industrial Control Systems (ICS), is widely used by water and sewage systems, power stations, oil refineries, chemical plants and other vital industrial infrastructure in the U.S. and around the world.

ICS increasingly has been the target of hackers since the Stuxnet cyber attack crippled the Iranian nuclear program in 2009.

"We've been advised that there may have been a cyber attack against our SCADA system," Donald M. Craven, one of seven elected trustees of the Curran-Gardner Public Water District near Springfield, told The Times on Sunday.

The Department of Homeland Security and the FBI "are gathering facts surrounding the [Illinois] report," Homeland Security spokesman Peter Boogaard said Friday. "At this time, there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety."

"I dislike, immensely, how the DHS tend to downplay how absolutely [expletive] the state of national infrastructure is," Pr0f responded.

A Homeland Security Department spokesman had no immediate response to Pr0f's comments.

Rep. James R. Langevin, Rhode Island Democrat and a member of the House Permanent Select Intelligence Committee, predicted more and worse cyber attacks on civilian U.S. infrastructure.

"These sorts of incidents are only going to become more and more common as we delay necessary reforms that would make our SCADA systems more secure," he said.

Mr. Langevin told The Times that the owners and operators of U.S. water and power systems and other infrastructure are "dragging their feet in terms of improving their computer security" to protect their systems from hacking.
Whatever the truth of the Illinois and Texas incidents, "We know this can be done," he

said, describing it as "massive risk we're facing as a country."

The Illinois report says the hackers likely had access to the system for several weeks. The attackers got access using passwords stolen from a company that sells ICS, meaning that other systems across the country also might be vulnerable to the hackers, according to SCADA security specialist Joseph Weiss, who first made the Illinois report public.

"This is a giant issue for the SCADA community," said Air Force Lt. Robert M. Lee, who has worked on SCADA cyber security issues.

If the Illinois report is correct, the attackers "created the same outcome that the Stuxnet achieved with Iranian centrifuges," he said.

The Stuxnet attack destroyed hundreds of Iran's uranium-enriching centrifuges by making the SCADA system spin them at ever-higher speeds until they shook to pieces.

"If I'm a foreign intelligence service, looking for ways to attack U.S. infrastructure," Lt. Lee said, "I'm going to do my homework, my intelligence gathering, in a smaller utility" like Curran-Gardner, where it is less likely to be noticed.

Mr. Langevin said it is "more likely than not" that the U.S. would "suffer a major cyber attack [on critical infrastructure] in the near future.

"We're very, very vulnerable if we don't act," he said.

**From Homeland1Newsletter, November 22, 2011*

May this holiday season be filled with good health, quality time with family, and the promise of a peaceful, more prosperous 2012!