Brennan Center Provides Resources for Security Activists

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of my constant themes to students (and to readers) is that security professionals ought to apply our knowledge of security fundamentals and technology to all aspects of our lives, including our roles as citizens. Here in the United States, one of the areas where I have personally contributed my perspective as a professional in the public sphere is discussions of electronic voting systems. As I have written in previous columns over the years (see for example http://www.networkworld.com/newsletters/sec/2003/0127sec1.html, http://www.networkworld.com/newsletters/sec/2003/0127sec2.html, and http://www.networkworld.com/newsletters/sec/2006/1009sec1.html), I profoundly object to electronic-voting systems that have no independently-verifiable audit trail; I’ve testified to that effect before the Vermont Senate, in public meetings on the issue, and in briefings presented to the office of the Secretary of State of Vermont.

On this theme of public involvement, I want to draw readers’ attention to an excellent resource that touches on many aspects close to our professional interests: the Brennan Center for Justice of the New York University School of Law. <http://www.brennancenter.org/> The Center has many areas of possible interest, including

- Access to Justice
- Campaign Finance Reform
- Courts & Government
- Immigrant Rights
- Liberty & National Security*
- Criminal Justice Reforms*
- Voting Rights & Elections*
- Wages, Jobs & a Strong Economy.

However, readers of this column may be particularly interested in the resources in the three sections I have marked with an asterisk.

In the “Liberty & National Security” page <http://www.brennancenter.org/subpage.asp?key=125&proj_key=54> the Center has links to many valuable documents discussing security implications of issues such as the abrogation of habeas corpus, the implications of unchecked presidential power, reduced independence of the federal courts, increased governmental secrecy, and racial and ethnic profiling.

The “Criminal Justice Reforms” section <http://www.brennancenter.org/subpage.asp?key=41> has a number of areas of possible interest to security practitioners, especially those with experience in or ties to law enforcement. Topics where security experts may be particularly interesting in contributing their expertise include

- Sentencing reform <
http://www.brennancenter.org/subpage.asp?key=42&proj_key=35685>, where one can read about attempts to “promote rational sentencing approaches through law reform that secures both fairness and safety” and which may help us reduce recidivism and the dangers posed by habitual offenders.

- Post-conviction penalties <http://www.brennnancenter.org/subpage.asp?key=42&proj_key=59> which examines to what degree offenders should continue to carry the stigmata of their crimes after their sentences are complete. These issues significantly affect our hiring policies and practices.

“Voting Rights & Elections” <http://www.brennancenter.org/subpage.asp?key=38&proj_key=76> is potentially the most interesting to technically-savvy security experts. There’s a comprehensive report available that appeared in October 2006 called “The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost” <http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf> that packs in 190 pages of detailed analysis of all aspects of electronic voting systems (watch out for the violently red page 2, which practically burst my eyeballs when I switched past it the first time). I was particularly pleased to see a section entitled “Voting System Vulnerabilities” that defined threat analysis and then went into several pages of details of potential attacks on voting systems. The six security recommendations are interesting and I encourage readers to study them in detail:

1. Conduct Automatic Routine Audit of Paper Records
2. Conduct Parallel Testing
3. Ban Wireless Components on All Voting Machines
4. Mandate Transparent and Random Selection Procedures
5. Ensure Decentralized Programming and Voting System Administration
6. Implement Effective Procedures for Addressing Evidence of Fraud or Error

In summary, there’s plenty of material on the Brennan Center’s site for anyone to study. Whether you agree with the Brennan Center’s positions, I hope that some readers will be motivated to get involved in their local, state and national affairs to contribute their intelligence and expertise.

* * *

Special discount for Network World Security Strategies readers: For a 10% discount on the upcoming INFOSEC Year in Review workshop <http://www.itpg.org/events_infosec.htm> in Marina Del Ray, CA on June 4-5, 2007, use code WNW07 when registering online or by phone.

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msi.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.