



By Lt. Gen. Harry D. Raduege Jr., USAF (Ret.)

“**N**early every day our nation is discovering new threats and attacks against our country’s networks. Inadequate cybersecurity and loss of information has inflicted unacceptable damage to U.S. economic and national security.” That is the sobering assessment recently provided to Congress by the Commission on Cybersecurity for the 44th Presidency sponsored by the Center for Strategic and International Studies.

national security problems facing the United States.

We are a nation increasingly dependent on the interconnectedness of information technology in every aspect of our lives. Our ability as a world economic power depends on the ability to securely conduct billions of dollars in financial transactions across the globe in milliseconds. Our military cannot go to war and win without the capability to link a variety of systems together and rapidly

breaches at the end of 2008, reflecting an increase of 47 percent over last year’s total of 446. The growing and ubiquitous use of mobile storage devices like laptops and thumb drives is only going to make the problem worse, unless security is the foremost concern.

The threat associated with the loss of sensitive information can be mitigated with appropriate cybersecurity controls. In the CSIS report, there were a series of important recommendations to improve

the overall cybersecurity situation of federal networks and critical infrastructure.

These recommendations

spanned several dimensions, ranging from new government organizational structures to improving the educational system of our country. In the context of public health and human service organizations there are two areas that deserve close attention:

- ♦ Identity Management — “The United States should make strong authentication of identity, based on robust in-person proofing and thorough verification of devices, a mandatory requirement for critical cyber infrastructure.”
- ♦ Privacy — Privacy and confidentiality are central values that any government cybersecurity initiative must respect. For authentication systems to be widely adopted, privacy concerns must be addressed.”

These two recommendation areas must be at the forefront of efforts to modernize public human service systems. Public- and private-sector networks are under relentless assault. The cyber threat targeting our networks is aggressive, sophisticated and persistent. These same threats are targeting public health and human systems for a variety of purposes, none of which are good. Public human service leaders must devote personal attention

See *Technology Speaks* on page 37

Cyber Threats May Be Hazardous to Your Privacy

The commission report, along with testimony from numerous government officials, confirms that cyber threats are targeting our public- and private-sector networks on a continuous basis. While generally acknowledged that such activities have probably been going on for years, only recently have senior leaders throughout government begun to realize the magnitude of the problem and begun to take action. Most recently, President Obama has declared that cybersecurity is a national priority and ordered a 60-day review of the nation’s cybersecurity to examine how federal agencies use technology to protect secrets and data. But what does all this really mean and what are the implications for public health and human service organizations?

The CSIS Cybersecurity Commission was a unique, year-long study that recently concluded this past December with the release of its final report, *Securing Cyberspace for the 44th Presidency*. The commission brought together an impressive group of experts from both the private and public sectors to study this complex problem and develop recommendations for a comprehensive strategy to improve cybersecurity in federal systems and in critical infrastructure. One of the three main findings of the commission was: Cybersecurity is now one of the major

share critical information. And, industry depends on IT networks for optimized services and competitive advantage. So, it’s no surprise that human service programs are increasingly using advanced technology, including networking connectivity, to dramatically improve services while gaining significant business efficiencies. However, there are also tremendous risks in how new IT systems and services are implemented and managed. And few areas of the government directly touch as many citizens at state and local levels as do our human service programs and systems.

There are a variety of cyber threats that are seeking opportunities to compromise any vulnerable network and access private information. The actors behind these threats range from hackers motivated by curiosity and the challenge, to sophisticated cyber criminals driven by profit, to well-resourced espionage organizations. Sensitive information on individuals can be exploited in a multitude of ways that include identity theft, fraud, financial compromise, and even something known as “social engineering” where personal data can be used to further access other types of personal information either electronically or in person. Reports of data breaches increased dramatically in 2008. The Identity Theft Resource Center’s 2008 breach report reached 656 reported

NSDTA

National Staff Development and Training Association
an affiliate of the American Public Human Services Association

Certification for Human Service Training and Development Professionals

The National Staff Development and Training Association announces planned piloting of certification for training and development professionals in human service fields. The Human Service Training and Development credential will be available in two states (California and Texas) beginning July 1, 2009 via several pathways:

1. Grandfathering experienced human service training and development practitioners (for a period of three years, ending July 1, 2012), contingent upon documentation of competence in at least one of the nine NSDTA roles and competence in a human services field (e.g., child protective services, child and youth work).
2. Completing formal training beyond the bachelor's level (e.g., master's level or postgraduate certificate) in training and development and documented competence in a human service field.
3. Completing a NSDTA approved (18-month) human service training and development certificate program and documented competence in a human service field.

Look for specific requirements regarding each option and additional information regarding certification on the NSDTA web site <http://nsdta.aphsa.org> or contact the Certification Committee chair, Dale Curry, dcurry@kent.edu or (330) 672-2998.

NAPIPM

National Association for Program Information and Performance Measurement
an affiliate of the American Public Human Services Association

What Has NAPIPM Got To Do With My State?

The National Association for Program Information and Performance Measurement serves as a forum for sharing states' mutual concerns regarding program integrity, quality control, quality assurance and process improvement. In this capacity, NAPIPM members work with TANF and the Improper Payments Information Act of 2002 audits.

The NAPIPM partnered with APHSA and the National Association of State TANF Administrators to raise concerns with OMB and HHS about whether a TANF National Payment Error Rate, based only on eight states, was reflective of the TANF goals Congress has set for states. APHSA, NASTA and NAPIPM questioned the audit methodology, which was based on each state's rules and included total ineligibility for cases where documentation was missing from case files. An alternative review method based on TANF factors common to all states was proposed. Concerns were raised with the federal agency administrators and visits were made to Capitol Hill to discuss this issue with legislators.

NAPIPM members work routinely with TANF, SNAP, Medicaid, CHIP, LIHEAP and Child Care programs. To find out how to contact your NAPIPM regional representative or to send us an e-mail with questions, comments or concerns, visit our web site at <http://www.napipm.org>.

Business News

from page 27

sive, efficient and consistent client interactions.

One of the greatest challenges facing agencies that administer child care programs is the management and oversight of providers required to support the program, meet increasing demand, and reach a broad geography. According to U.S. Administration for Children and Families, there are more than 665,529 providers across the United States providing child care services that have to be supported by an ever-reducing number of staff. Cúram for Child Care delivers:

- ♦ Extensive provider self-service capabilities to reduce staff workload
- ♦ Electronic financial management to reduce inefficiencies and cost
- ♦ Convenient provider search and matching to improve service quality
- ♦ Comprehensive place management to enhance child care quality
- ♦ Simplified tracking of accreditation, license, contracts and background checks leading to better provider quality.

Technology Speaks

from page 24

to this issue and make certain that IT investments include a strong, viable cybersecurity dimension that focuses on identity management and privacy. Without this awareness and commitment, our well-being, health and security are in jeopardy. We owe it to every member of society we serve.

Harry D. Raduege Jr. is the chairman of the Deloitte Center for Network Innovation. He served in the U.S. Air Force for over 35 years in various key senior leadership positions involving information technology, satellite communications, network operations and cybersecurity.